

Triviality Theorems for Yetter-Drinfel'd Hopf Algebras

Yorck Sommerhäuser

Abstract

Under suitable assumptions on the base field, we prove that a commutative semisimple Yetter-Drinfel'd Hopf algebra over a finite abelian group is trivial, i.e., is an ordinary Hopf algebra, if its dimension is relatively prime to the order of the finite abelian group. Furthermore, we prove that a finite-dimensional cocommutative cosemisimple Yetter-Drinfel'd Hopf algebra contains a trivial Yetter-Drinfel'd Hopf subalgebra of dimension greater than one, at least if the Yetter-Drinfel'd Hopf algebra itself has dimension greater than one.

Introduction

Usually, a Yetter-Drinfel'd Hopf algebra is not an ordinary Hopf algebra. The difference between the two notions is caused by the fact that the coproduct of a Yetter-Drinfel'd Hopf algebra is not an algebra homomorphism with respect to the canonical algebra structure on the second tensor power of the Yetter-Drinfel'd Hopf algebra. Rather, it is an algebra homomorphism with respect to a modified algebra structure on the second tensor power constructed via a special quasisymmetry that is characteristic for Yetter-Drinfel'd modules. However, it may happen that, for the specific Yetter-Drinfel'd Hopf algebra under consideration, this quasisymmetry coincides on the second tensor power of the algebra with the ordinary flip of tensor factors. Then the algebra structure is in fact not modified, and the Yetter-Drinfel'd Hopf algebra is an ordinary Hopf algebra.

In this case, the Yetter-Drinfel'd Hopf algebra is called trivial (cf. [30], Def. 1.1, p. 8). According to a result of P. Schauenburg, the behavior of the quasisymmetry just described characterizes this property: If a Yetter-Drinfel'd Hopf algebra is an ordinary Hopf algebra, then the quasisymmetry for Yetter-Drinfel'd modules coincides on the second tensor power of the algebra with the ordinary flip of tensor factors (cf. [25], Cor. 2, p. 262; see also [30], Prop. 1.1, p. 8).

The first main result of this article is that, in a certain situation, every Yetter-Drinfel'd Hopf algebra is trivial. In this situation, we consider a semisimple

commutative Yetter-Drinfel'd Hopf algebra A over the group ring $K[G]$ of a finite abelian group G , where K is a field of characteristic zero, and prove in Paragraph 3.9 the following triviality theorem:

Theorem If $\dim(A)$ and $|G|$ are relatively prime, then A is trivial.

This result was known in the case where $|G|$ is prime (cf. [30], Cor. 6.7, p. 100).

The second main result of this article is concerned with a finite-dimensional cocommutative cosemisimple Yetter-Drinfel'd Hopf algebra A over the group ring $K[G]$ of a finite abelian group G , where K is an algebraically closed field of characteristic zero. We also prove in Paragraph 3.9 that, although A itself need not be trivial, it contains at least a trivial part:

Proposition If $\dim(A) > 1$, then A contains a trivial Yetter-Drinfel'd Hopf subalgebra B with $\dim(B) > 1$.

We develop the rather involved general theory of such Yetter-Drinfel'd Hopf algebras here only to the extent that is necessary to prove these two results. Section 1 contains a brief, but nonetheless very important, summary of basic facts about Yetter-Drinfel'd Hopf algebras. More detailed treatments of this material can be found in [26], [27], [28], [29], or [30]. Section 1 ends with Theorem 1.5, a version of the Nichols-Zoeller theorem for two Yetter-Drinfel'd Hopf algebras that are not necessarily defined over the same Hopf algebra. In Section 2, we discuss Yetter-Drinfel'd Hopf algebras over group rings of finite abelian groups. In particular, we introduce there a certain alternative description of the coaction that will be used in the entire article. This brief section also contains an important discussion of a way to modify the finite abelian group over which the Yetter-Drinfel'd Hopf algebra is defined. The main part of the article is Section 3, which deals with commutative semisimple Yetter-Drinfel'd Hopf algebras over group rings of finite abelian groups. As we will indicate during the discussion, most of the material presented there generalizes facts that were established in Chapter 6 of [30] for the case in which the finite abelian group has prime order. This final section of the article ends with the proof of the two main results stated above.

While the precise assumptions that are used throughout each section are listed in its first paragraph, there are some conventions that are common to all sections. The base field is always denoted by K , and while it is arbitrary in Section 1, we assume that it is algebraically closed of characteristic zero in Section 2 and Section 3 unless this is explicitly stated otherwise, which happens only in a minor comment in Paragraph 3.9. The multiplicative group of invertible elements in the field K is denoted by $K^\times := K \setminus \{0\}$. All vector spaces are defined over K , and all unadorned tensor products are taken over K . The dual of a vector space V is denoted by $V^* := \text{Hom}_K(V, K)$, and the transpose of a linear map f , i.e., the induced map between the dual spaces, is denoted by f^* . The symbol \perp will be

used in four different meanings, two for vector spaces and two for groups. In this article, a character is a one-dimensional character, i.e., a group homomorphism to the multiplicative group K^\times in the case of a group character, or an algebra homomorphism to the base field K in the case of the character of an algebra. All rings, and therefore especially all algebras, are assumed to have a unit element, and ring and algebra homomorphisms are assumed to preserve unit elements. Unless stated otherwise, a module is a left module. The cardinality of a set X is denoted by $|X|$. The symbol \subset denotes non-strict inclusion, so that we have $X \subset X$ for every set X . Also, we use the so-called Kronecker symbol δ_{ij} , which is equal to 1 if $i = j$ and equal to 0 otherwise. With respect to enumeration, we use the convention that propositions, definitions, and similar items are referenced by the paragraph in which they occur; i.e., a reference to Proposition 1.1 refers to the unique proposition in Paragraph 1.1.

The first main result of this article was presented at the AMS Fall Eastern Sectional Meeting in Halifax in October 2014, while the second main result was presented at the Joint Mathematics Meeting in San Antonio in January 2015. The author thanks the organizers of these conferences for the invitation. He also thanks the Department of Mathematics at SUNY Buffalo for a visiting appointment during which most of this article was written.

1 Preliminaries

1.1 Although we will limit our considerations to special situations soon, let us briefly recall the case of a general Hopf algebra H with coproduct Δ_H , counit ε_H , and antipode S_H . A left-left Yetter-Drinfel'd module, or left Yetter-Drinfel'd module for short, is a left H -module V that is simultaneously a left H -comodule in such a way that these two structures are compatible in the sense that

$$\delta(h.v) = h_{(1)}v^{(1)}S_H(h_{(3)}) \otimes h_{(2)}.v^{(2)}$$

for all $h \in H$ and all $v \in V$. Here we have used Heyneman-Sweedler sigma notation in the form

$$\Delta_H(h) = h_{(1)} \otimes h_{(2)} \in H \otimes H \quad \delta(v) = v^{(1)} \otimes v^{(2)} \in H \otimes V$$

for the coproduct Δ_H and the coaction δ , respectively. The dot denotes the module action. Although right Yetter-Drinfel'd modules will be defined below, we always mean left Yetter-Drinfel'd modules if no side is specified. We note already at this point that, in the case where H is commutative and cocommutative, which will be the case in Section 2 and Section 3, the Yetter-Drinfel'd condition stated above reduces to

$$\delta(h.v) = v^{(1)} \otimes h.v^{(2)}$$

which coincides with the compatibility condition for left-left dimodules (cf. [16], Def. 3.1, p. 575).

The base field K is a Yetter-Drinfel'd module if endowed with the trivial module structure $h.\xi := \varepsilon_H(h)\xi$ and the trivial comodule structure $\delta(\xi) := 1_H \otimes \xi$, for $\xi \in K$. Moreover, the tensor product of two Yetter-Drinfel'd modules, together with the usual diagonal module structure and the codiagonal comodule structure, is again a Yetter-Drinfel'd module. If V and W are two Yetter-Drinfel'd modules, the two possible ways of forming their tensor product are related via the quasisymmetry

$$\sigma_{V,W} : V \otimes W \rightarrow W \otimes V, \quad v \otimes w \mapsto (v^{(1)}.w \otimes v^{(2)})$$

This map is both H -linear and colinear. If the antipode of H is bijective, the quasisymmetry is also bijective, and its inverse is then given by the formula $\sigma_{V,W}^{-1}(w \otimes v) = v^{(2)} \otimes S_H^{-1}(v^{(1)}).w$.

1.2 Similarly, a right-right Yetter-Drinfel'd module, or right Yetter-Drinfel'd module for short, is a right H -module V that is simultaneously a right H -comodule in such a way that these two structures are compatible in the sense that

$$\delta(v.h) = v^{(1)}.h_{(2)} \otimes S_H(h_{(1)})v^{(2)}h_{(3)}$$

for all $h \in H$ and all $v \in V$. It is important to note that here, in contrast to the previous case, $v.h \in V$ and $\delta(v) = v^{(1)} \otimes v^{(2)} \in V \otimes H$. As right H -modules are just left modules over the opposite algebra H^{op} and right H -comodules are just left comodules over the coproduct coalgebra H^{cop} , right Yetter-Drinfel'd modules over H are just left Yetter-Drinfel'd modules over $H^{\text{op cop}}$. It is also possible to define left-right and right-left Yetter-Drinfel'd modules, but they will not be used in the sequel. As before, in the case where H is commutative and cocommutative, the right Yetter-Drinfel'd condition coincides with the right-right dimodule condition

$$\delta(v.h) = v^{(1)}.h \otimes v^{(2)}$$

Again, the base field K is a right Yetter-Drinfel'd module if endowed with the trivial module structure $\xi.h := \varepsilon_H(h)\xi$ and the trivial comodule structure $\delta(\xi) := \xi \otimes 1_H$, for $\xi \in K$, and the tensor product of two right Yetter-Drinfel'd modules V and W , together with the usual diagonal module structure and the codiagonal comodule structure, is again a right Yetter-Drinfel'd module. The formula for the quasisymmetry is $\sigma_{V,W}(v \otimes w) = w^{(1)} \otimes v.w^{(2)}$ in this case. As before, the quasisymmetry is bijective with inverse

$$\sigma_{V,W}^{-1}(w \otimes v) = v.S_H^{-1}(w^{(2)}) \otimes w^{(1)}$$

if the antipode S_H is bijective. It should be noted that it is necessary to reverse the tensor factors when considering right Yetter-Drinfel'd modules as left Yetter-Drinfel'd modules over $H^{\text{op cop}}$: If the right Yetter-Drinfel'd modules V and W are viewed as left Yetter-Drinfel'd modules over $H^{\text{op cop}}$, their tensor product $V \otimes W$ over $H^{\text{op cop}}$ does not correspond to their tensor product $V \otimes W$

over H , but rather to the tensor product $W \otimes V$ over H , viewed as a left Yetter-Drinfel'd module over $H^{\text{op cop}}$. This reversion of the tensor factors is also compatible with the quasisymmetries. In the language of category theory, this means that we have constructed a (non-strict) quasisymmetric monoidal functor from the category of right Yetter-Drinfel'd modules over H to the reverse category of the category of left Yetter-Drinfel'd modules over $H^{\text{op cop}}$ (cf. [10], Ex. 2.5, p. 39; [11], Exerc. XIII.6.4, p. 337).

In our treatment, right Yetter-Drinfel'd modules arise as duals of left Yetter-Drinfel'd modules as a consequence of the following proposition:

Proposition If V is a finite-dimensional left Yetter-Drinfel'd module, then the dual space V^* is in a unique way a right Yetter-Drinfel'd module such that the natural pairing

$$\langle \cdot, \cdot \rangle : V \times V^* \rightarrow K, (v, \varphi) \mapsto \langle v, \varphi \rangle := \varphi(v)$$

is a Yetter-Drinfel'd form in the sense that we have

1. $\langle h.v, \varphi \rangle = \langle v, \varphi.h \rangle$
2. $\langle v, \varphi^{(1)} \rangle \varphi^{(2)} = v^{(1)} \langle v^{(2)}, \varphi \rangle$

If W is another finite-dimensional left Yetter-Drinfel'd module, then the pairing between $V \otimes W$ and $V^* \otimes W^*$ defined by

$$\langle v \otimes w, \varphi \otimes \varphi' \rangle = \langle v, \varphi \rangle \langle w, \varphi' \rangle$$

is also a Yetter-Drinfel'd form, and the quasisymmetries are mutually adjoint with respect to this pairing; i.e., we have

$$\langle \sigma_{V,W}(v \otimes w), \varphi' \otimes \varphi \rangle = \langle v \otimes w, \sigma_{W^*,V^*}(\varphi' \otimes \varphi) \rangle$$

for $v \in V$, $w \in W$, $\varphi \in V^*$, and $\varphi' \in W^*$. In the language of category theory, this means that we have constructed a (non-strict) quasisymmetric monoidal functor from the category of finite-dimensional left Yetter-Drinfel'd modules to the category of finite-dimensional right Yetter-Drinfel'd modules. More precisely, since this functor is contravariant, it is a functor to the opposite category of the category of finite-dimensional right Yetter-Drinfel'd modules (cf. [34], Thm. II.5.4, p. 112). Proofs of these statements, which are not difficult, are briefly indicated in [27], Subsec. 2.4 and Subsec. 2.5, p. 37; more detailed proofs can be found in the corresponding parts of [26].

1.3 A left (or right) Yetter-Drinfel'd algebra is a left (or right) Yetter-Drinfel'd module which is simultaneously an associative algebra with unit in such a way that the multiplication map

$$\mu_A : A \otimes A \rightarrow A, a \otimes a' \mapsto aa'$$

and the unit map $K \rightarrow A$, $\xi \mapsto \xi 1_A$ are both H -linear and colinear. If A' is a second left (or right) Yetter-Drinfel'd algebra, then the tensor product $A \otimes A'$ becomes an associative algebra with unit with respect to the multiplication

$$\mu_{A \otimes A'} := (\mu_A \otimes \mu_{A'}) \circ (\text{id}_A \otimes \sigma_{A' \otimes A} \otimes \text{id}_{A'})$$

The difference to the canonical tensor algebra structure consists in the fact that this algebra structure uses the quasisymmetry $\sigma_{A' \otimes A}$ instead of the usual flip of tensor factors. We denote this tensor product by $A \hat{\otimes} A'$ if we want to emphasize that it carries this algebra structure in contrast to the canonical tensor algebra structure. For left Yetter-Drinfel'd algebras, the explicit form of this product is

$$(a \otimes a')(b \otimes b') = a(a'^{(1)}.b) \otimes a'^{(2)}b'$$

which shows that this multiplication is a special case of a left smash product of the module algebra A and the comodule algebra A' (cf. [2], Def. 1.2, p. 24; see also [4], Rem. (1.3), p. 374 and [30], Par. 1.7, p. 15).

Analogously, a left (or right) Yetter-Drinfel'd coalgebra is a left (or right) Yetter-Drinfel'd module which is simultaneously a coalgebra in such a way that the comultiplication $\Delta_A : A \rightarrow A \otimes A$ and the counit $\varepsilon_A : A \rightarrow K$ are both H -linear and colinear. A left (or right) Yetter-Drinfel'd bialgebra is a left (or right) Yetter-Drinfel'd algebra which is simultaneously a Yetter-Drinfel'd coalgebra with the property that both the coproduct Δ_A and the counit ε_A are algebra homomorphisms. Here, when we say that Δ_A is an algebra homomorphism, we refer to the algebra structure $A \hat{\otimes} A$ described above, and not to the canonical tensor algebra structure; i.e., we view the coproduct as a map $\Delta_A : A \rightarrow A \hat{\otimes} A$. Finally, a left (or right) Yetter-Drinfel'd Hopf algebra is a left (or right) Yetter-Drinfel'd bialgebra together with an H -linear and colinear map $S_A : A \rightarrow A$, called the antipode, that satisfies

$$S_A(a_{(1)})a_{(2)} = a_{(1)}S_A(a_{(2)}) = \varepsilon_A(a)1_A$$

for all $a \in A$. As in the case of ordinary Hopf algebras, such an antipode satisfies $S_A(1_A) = 1_A$ and $\varepsilon_A \circ S_A = \varepsilon_A$, but in the compatibility with product and coproduct the flip of tensor factors must again be replaced by the quasisymmetry, namely in the form

$$S_A \circ \mu_A = \mu_A \circ (S_A \otimes S_A) \circ \sigma_{A,A} \quad \Delta_A \circ S_A = \sigma_{A,A} \circ (S_A \otimes S_A) \circ \Delta_A$$

(cf. [17], Prop. 3.1, p. 270; [19], § 10.5, Eq. (10.5.9), p. 205; [28], Par. 2.5, p. 427). As for Hopf algebras, the antipode of a finite-dimensional Yetter-Drinfel'd Hopf algebra is bijective (cf. [5], Thm. 3, p. 3066; [28], Prop. 2.10, p. 432).

It is obvious from our definitions that a Yetter-Drinfel'd Hopf algebra is in general not an ordinary Hopf algebra, because the algebra structure on $A \hat{\otimes} A$ is in general different from the canonical tensor algebra structure. However, it is also obvious from our definitions that these two algebra structures coincide

if it happens that $\sigma_{A \otimes A}(a \otimes a') = a' \otimes a$ for all $a, a' \in A$, in which case A is indeed an ordinary Hopf algebra. As observed by P. Schauenburg, the converse of this statement is also true: If a Yetter-Drinfel'd Hopf algebra is an ordinary Hopf algebra, then we have $\sigma_{A \otimes A}(a \otimes a') = a' \otimes a$ for all $a, a' \in A$ (cf. [25], Cor. 2, p. 262; see also [30], Prop. 1.1, p. 8). We call such Yetter-Drinfel'd Hopf algebras trivial:

Definition A left (or right) Yetter-Drinfel'd Hopf algebra A is called trivial if we have $\sigma_{A,A}(a \otimes a') = a' \otimes a$ for all $a, a' \in A$.

One of the main results of this article, namely Theorem 3.9, describes a situation that forces a Yetter-Drinfel'd Hopf algebra to be trivial.

We have already discussed in Paragraph 1.2 how the dual space of a finite-dimensional left Yetter-Drinfel'd module becomes a right Yetter-Drinfel'd module. If the left Yetter-Drinfel'd module was a Yetter-Drinfel'd Hopf algebra, the arising right Yetter-Drinfel'd module is also a Yetter-Drinfel'd Hopf algebra:

Proposition If A is a finite-dimensional left Yetter-Drinfel'd Hopf algebra, then the dual space A^* is in a unique way a right Yetter-Drinfel'd Hopf algebra such that the natural pairing described above is not only a Yetter-Drinfel'd form, but also a bialgebra form, which means that we have

1. $\langle a \otimes a', \Delta_{A^*}(\varphi) \rangle = \langle aa', \varphi \rangle$
2. $\langle a, \varphi\varphi' \rangle = \langle \Delta_A(a), \varphi \otimes \varphi' \rangle$
3. $\langle 1_A, \varphi \rangle = \varepsilon_{A^*}(\varphi), \langle a, 1_{A^*} \rangle = \varepsilon_A(a)$

where the pairing of the second tensor powers is defined as in Paragraph 1.2.

This proposition appears in several places, among them [27], Subsec. 2.6, p. 37; the corresponding part of [26] contains further details. More material about Yetter-Drinfel'd Hopf algebras can be found in [19], [22], [28], or [30], and some of the results established there will be used in the sequel.

We have also discussed in Paragraph 1.2 that right Yetter-Drinfel'd modules over H are just left Yetter-Drinfel'd modules over $H^{\text{op cop}}$, up to a reversion of the order of tensor products. For Yetter-Drinfel'd Hopf algebras, this implies the following:

Lemma

1. If A is a left Yetter-Drinfel'd Hopf algebra over H , then the opposite algebra and coopposite coalgebra $A^{\text{op cop}}$ is a right Yetter-Drinfel'd Hopf algebra over $H^{\text{op cop}}$.
2. If A is a right Yetter-Drinfel'd Hopf algebra over H , then $A^{\text{op cop}}$ is a left Yetter-Drinfel'd Hopf algebra over $H^{\text{op cop}}$.

This result is already stated in [27], Lem. 2.4, p. 39; again, the corresponding part of [26] contains a slightly more detailed treatment. The result is also stated in [28], Lem. 2.5, p. 427 and [30], Lem. 1.2, p. 9.

1.4 In Proposition 1.2 and Proposition 1.3, we have dualized Yetter-Drinfel'd modules and Yetter-Drinfel'd Hopf algebras, respectively. But if the underlying Hopf algebra H is finite-dimensional, the process of dualization can also be applied to H : If H is finite-dimensional and V is a left Yetter-Drinfel'd module over H , we know from [19], Lem. 1.6.4, p. 11 that the left comodule structure determines a right H^* -module structure, namely the module structure

$$V \otimes H^* \rightarrow V, v \otimes \varphi \mapsto \varphi(v^{(1)})v^{(2)}$$

Dually, the left H -module structure determines a right H^* -comodule structure

$$\delta_* : V \rightarrow V \otimes H^*, v \mapsto v^{[1]} \otimes v^{[2]}$$

such that the analogous condition $(v^{[2]}(h))v^{[1]} = h.v$ is satisfied for all $v \in V$ and $h \in H$, where we have used square brackets to distinguish the H^* -coaction from the H -coaction. It is then straightforward to verify that V is a right Yetter-Drinfel'd module over H^* .

By construction, a mapping between two Yetter-Drinfel'd modules is linear and colinear with respect to H if and only if it is linear and colinear with respect to H^* . This dualization process commutes with taking the tensor product of two Yetter-Drinfel'd modules, and the quasisymmetry on the tensor product is the same before and after the dualization, because the preceding compatibility conditions imply that

$$w^{[1]} \otimes v.w^{[2]} = w^{[1]} \otimes w^{[2]}(v^{(1)})v^{(2)} = v^{(1)}.w \otimes v^{(2)}$$

for elements of two left Yetter-Drinfel'd modules V and W . In the language of category theory, this means that we have constructed a strict quasisymmetric monoidal functor from the category of left Yetter-Drinfel'd modules over H to the category of right Yetter-Drinfel'd modules over H^* . Therefore, if A is a left Yetter-Drinfel'd Hopf algebra over H , it can also be considered as a right Yetter-Drinfel'd Hopf algebra over H^* . Similarly, if A is a right Yetter-Drinfel'd Hopf algebra over H , it can also be considered as a left Yetter-Drinfel'd Hopf algebra over H^* , as can be deduced from Lemma 1.3. This topic is also discussed in [28], Lem. 2.4, p. 427 and [30], Lem. 1.3, p. 10.

1.5 We will need some results from the theory of integrals for Yetter-Drinfel'd Hopf algebras. The basic facts about integrals for Yetter-Drinfel'd Hopf algebras were already obtained by D. E. Radford in [21], although some results there were proved only under the additional assumption that the Yetter-Drinfel'd Hopf algebra is an ordinary Hopf algebra; i.e., that it is trivial in the sense of

Definition 1.3. The theory was afterwards developed further by several authors, for example in the articles [5], [7], [17], [18], and [28]. Here, we only briefly collect those results that will become relevant in the sequel, following the treatment in [28]:

Proposition Suppose that A is a semisimple left Yetter-Drinfel'd Hopf algebra over the semisimple Hopf algebra H , and that the base field K has characteristic zero. Then the following holds:

1. There is a unique two-sided integral $\Lambda_A \in A$ satisfying $\varepsilon_A(\Lambda_A) = 1$.
2. There is a unique two-sided integral $\lambda_A \in A^*$ satisfying $\lambda_A(\Lambda_A) = 1$.
3. A is finite-dimensional.
4. λ_A is the character of the regular representation.
5. $\lambda_A(1_A) = \dim(A)$
6. $S_A(\Lambda_A) = \Lambda_A$ and $\lambda_A \circ S_A = \lambda_A$
7. λ_A is a Frobenius homomorphism with corresponding Casimir element

$$\Lambda_{A(1)} \otimes S_A(\Lambda_{A(2)}) = S_A(\Lambda_{A(1)}) \otimes \Lambda_{A(2)}$$

i.e., we have $a = \lambda_A(a\Lambda_{A(1)})S_A(\Lambda_{A(2)}) = S_A(\Lambda_{A(1)})\lambda_A(\Lambda_{A(2)}a)$ for all $a \in A$.

8. λ_A and Λ_A are cocommutative.

Proof. (1) The kernel of ε_A is a two-sided ideal of codimension 1. Since A is semisimple, there is a two-sided ideal that complements this kernel; this complement is then one-dimensional. As in the case of Maschke's theorem for ordinary Hopf algebras (cf. [19], Thm. 2.2.1, p. 20; [22], Thm. 10.3.2, p. 298; [32], Thm. 5.1.8, p. 103), we can see that a nonzero element Λ_A in this complement is a two-sided integral. Since Λ_A is not contained in the kernel of ε_A , we have $\varepsilon_A(\Lambda_A) \neq 0$; via rescaling, we can achieve that $\varepsilon_A(\Lambda_A) = 1$. By multiplying Λ_A with a potentially different element with the same properties, we see that this element is unique, proving the first assertion.

(2) Since H is semisimple, H is finite-dimensional (cf. [22], Prop. 10.2.1, p. 293; [31], Cor. 2.7, p. 330; [32], Chap. V, Exerc. 4, p. 108). If $\Lambda_H \in H$ is a two-sided integral satisfying $\varepsilon_H(\Lambda_H) = 1$, then $\Lambda_B := \Lambda_A \otimes \Lambda_H$ is a right integral in the Radford biproduct $B := A \otimes H$ (cf. [21], Prop. 3, p. 333). Since $\varepsilon_A(\Lambda_A)\varepsilon_H(\Lambda_H) = 1$, the Radford biproduct is semisimple, and therefore finite-dimensional by the result just cited. But this obviously means that A is finite-dimensional, which proves the third assertion.

(3) Now we can choose nonzero right integrals $\lambda_A \in A^*$ and $\lambda_H \in H^*$ (cf. [5], Thm. 3, p. 3066; [7], Cor. 5.8, p. 4885; [28], Prop. 2.10, p. 432). Then the formula

$$\lambda_B(a \otimes h) = \lambda_A(a)\lambda_H(h)$$

defines a right integral λ_B on the Radford biproduct $B = A \otimes H$ (cf. [21], Prop. 4, p. 335). Since B is in this situation also cosemisimple (cf. [15], Thm. 3.3, p. 276), we have

$$\lambda_B(1_B) = \lambda_A(1_A)\lambda_H(1_H) \neq 0$$

and therefore $\lambda_A(1_A) \neq 0$ and $\lambda_H(1_H) \neq 0$. By rescaling λ_A and λ_H , we can achieve that $\lambda_A(1_A) = \dim(A)$ and $\lambda_H(1_H) = \dim(H)$. Therefore also A is cosemisimple and both λ_A and λ_H are two-sided integrals (cf. [28], Cor. 2.14, p. 438). Now it follows from [14], Thm. 4, p. 195 together with [15], Thm. 4.4, p. 279 that λ_B is the character of the (left or right) regular representation of B . Since $(a \otimes 1_H)(a' \otimes h') = aa' \otimes h'$, it follows that $\lambda_B(a \otimes 1_H)$ is $\dim(H)$ times the trace of the map $a' \mapsto aa'$. But since we clearly have $\lambda_B(a \otimes 1_H) = \lambda_A(a)\dim(H)$, this implies that this integral is the character of the regular representation. The fourth assertion will then follow if we can show that λ_A also satisfies the normalization condition given in the second assertion, which we do next.

(4) From the first step of this proof, we know that Λ_A is a centrally primitive idempotent that spans a one-dimensional two-sided ideal. It has therefore trace 1 in the regular representation. In view of the preceding step, this means that $\lambda_A(\Lambda_A) = 1$, proving the second assertion, as this normalization condition obviously determines the integral uniquely, and therefore also completing the proof of the fourth assertion.

(5) We have already obtained the fifth assertion in the proof of the fourth assertion above; it also follows immediately from the fourth assertion itself. In addition, it is a special case of a trace formula that appears in [1], Thm. 7.3, p. 445 and [28], Par. 3.11, p. 447.

(6) By [28], Prop. 2.12, p. 436, the antipode maps left integrals to right integrals and right integrals to left integrals. Since our integral is two-sided, $S_A(\Lambda_A)$ is proportional to Λ_A . But as we stated in Paragraph 1.3, we have $\varepsilon_A \circ S_A = \varepsilon_A$ and therefore $\varepsilon_A(S_A(\Lambda_A)) = \varepsilon_A(\Lambda_A) = 1$, which shows that the proportionality constant must be 1, so that $S_A(\Lambda_A) = \Lambda_A$. In view of Proposition 1.3 and Lemma 1.3, the equation $\lambda_A \circ S_A = \lambda_A$ follows by applying this result to A^* .

(7) The two forms of the Casimir element given in the seventh assertion follow from [28], Prop. 2.10, p. 432 and Prop. 4.2, p. 449, respectively, because in our case the integrals are two-sided and the integral character ι_A , the integral group element g_A , and the right modular element a_A^R used there are $\iota_A = \varepsilon_H$, $g_A = 1_H$, and $a_A^R = 1_A$ (cf. [28], Prop. 2.14 and Cor. 2.14, p. 438; see also [5], Thm. 3, p. 3066; [7], Thm. 5.6, p. 4883).

(8) For the eighth assertion, we note that the character of the regular representation is clearly cocommutative, so that λ_A is cocommutative by the fourth

assertion, i.e., satisfies $\lambda_A(ab) = \lambda_A(ba)$ for all $a, b \in A$. Alternatively, we know from [28], Thm. 4.5, p. 454 that the negatively twisted Nakayama automorphism coincides with the square S_A^2 of the antipode in our case, and then [28], Prop. 4.6, p. 455 shows that the ordinary Nakayama automorphism is the composition of S_A^2 with the ribbon transformation θ_A , defined in [28], Par. 3.5, p. 441. But from the references cited in the third step, we know that the semisimplicity and cosemisimplicity of the Radford biproduct $B = A \otimes H$ implies that the square of its antipode is the identity, which entails by [1], Eq. (4.4), p. 437 or [28], Prop. 3.11, p. 447 that $S_A^2 \circ \theta_A$ is the identity. Thus the (ordinary) Nakayama automorphism is the identity, which means that λ_A is cocommutative. By applying this result to A^* , we get in view of Proposition 1.3 and Lemma 1.3 that Λ_A is cocommutative, i.e., that $\Lambda_{A(1)} \otimes \Lambda_{A(2)} = \Lambda_{A(2)} \otimes \Lambda_{A(1)}$. \square

In the sequel, we will always use integrals that satisfy the two normalization conditions $\varepsilon_A(\Lambda_A) = 1$ and $\lambda_A(\Lambda_A) = 1$ appearing in this proposition. We note that the converse of its first assertion holds: If there exists a (left) integral Λ_A satisfying $\varepsilon_A(\Lambda_A) = 1$, then A is semisimple (cf. [28], Prop. 2.14, p. 438). This shows that A remains semisimple under extension of the base field; i.e., A is separable (cf. [3], Def. (7.1), p. 142).

The Nichols-Zoeller freeness theorem for ordinary Hopf algebras (cf. [19], Thm. 3.1.5, p. 30; [20], Thm. 7, p. 384; [22], Thm. 9.3.3, p. 281) has been generalized to Yetter-Drinfel'd Hopf algebras by B. Scharfschwerdt (cf. [24], Thm. 2.2, p. 2483; see also [23]; [1], Prop. 4.9, p. 438; [30], Prop. 1.8, p. 16). We give here a slightly different version in which the smaller Yetter-Drinfel'd Hopf algebra is not necessarily defined over the same Hopf algebra as the larger one:

Theorem For a base field K of characteristic zero, we consider a semisimple left Yetter-Drinfel'd Hopf algebra A over the semisimple Hopf algebra H that contains a unital subalgebra $B \subset A$ that is simultaneously a subcoalgebra. We assume that B is also a left Yetter-Drinfel'd Hopf algebra over a potentially different semisimple Hopf algebra H' . Then the following holds:

1. B is semisimple.
2. A is free as a left and right module over B .
3. $\dim(B)$ divides $\dim(A)$.

Proof. (1) In the third step of the proof of the preceding proposition, we have already described the integrals on the Radford biproduct $A \otimes H$, and the discussion there shows that the Radford biproduct $A \otimes H$ is cosemisimple if and only if its two factors A and H are cosemisimple. In the second step of this proof, we have also described the integrals in the Radford biproduct, and this description together with the first assertion of the proposition and its converse shows that the Radford biproduct $A \otimes H$ is semisimple if and only if its two factors A and H are semisimple. Analogous statements hold for B and H' .

Now it also follows from the discussion in the second and third step of the preceding proof that in characteristic zero a Hopf algebra is semisimple if and only if it is finite-dimensional and cosemisimple. Since both H and H' are semisimple by assumption, and therefore finite-dimensional and cosemisimple, we see first that A , which is also semisimple by assumption, is finite-dimensional and cosemisimple, and second that B is semisimple if and only if it is cosemisimple.

(2) Because B is a subcoalgebra of A , the restriction of the integral $\lambda_A \in A^*$ described above to B is still an integral on B . Because $1_A \in B$ by assumption and $\lambda_A(1_A) = \dim(A) \neq 0$, this restriction is nonzero, and B is cosemisimple by the version of Maschke's theorem for Yetter-Drinfel'd Hopf algebras in the third step of the preceding proof that we have already mentioned several times. As we saw in the first step, this implies that B is semisimple.

(3) We now consider the corresponding integrals $\lambda_B \in B^*$ and $\Lambda_B \in B$ for B , subject to the analogous normalization conditions $\varepsilon_B(\Lambda_B) = 1$ and $\lambda_B(\Lambda_B) = 1$. Because the spaces of integrals are one-dimensional (cf. [5], Thm. 3, p. 3066; [7], Cor. 5.8, p. 4885; [28], Prop. 2.10, p. 432), the restriction of the integral $\lambda_A \in A^*$ to B must be proportional to λ_B . Because $\lambda_A(1_A) = \dim(A)$ and $\lambda_B(1_A) = \dim(B)$ by the preceding proposition, we must have

$$\lambda_A|_B = \frac{\dim(A)}{\dim(B)} \lambda_B$$

which clearly implies

$$\lambda_A(\Lambda_B) = \frac{\dim(A)}{\dim(B)}$$

Since Λ_B is an idempotent and λ_A is, according to the preceding proposition, the character of the (left or right) regular representation, the left-hand side of this equation is an integer. This shows that $\dim(B)$ divides $\dim(A)$.

(4) If $l := \dim(A)/\dim(B)$, the above equality states that the restriction of the character of the (left or right) regular representation of A to B is l times the character of the (left or right) regular representation of B . This implies that

$$A \cong B^l$$

as (left or right) B -modules; in other words, A is free of rank l over B , as asserted. \square

It should be mentioned that there are other freeness results for Yetter-Drinfel'd Hopf algebras in the literature in which the smaller Yetter-Drinfel'd Hopf algebra is not necessarily defined over the same Hopf algebra as the larger Yetter-Drinfel'd Hopf algebra: Such results for Nichols algebras, which are certain special Yetter-Drinfel'd Hopf algebras, have been obtained by M. Graña (cf. [8], Thm. 3.8, p. 250).

2 Finite Abelian Groups

2.1 We now specialize the situation to the case where $H = K[G]$ is the group ring of a finite abelian group over an algebraically closed field K of characteristic zero. A left Yetter-Drinfel'd module V over H is in particular a module over H , and this module structure can be described equivalently by a representation

$$G \rightarrow \text{Aut}(V), g \mapsto \phi_g$$

of G . V is also a left comodule over H , i.e., a G -graded vector space (cf. [19], Ex. 1.6.7, p. 12), and as the Yetter-Drinfel'd condition reduces to the dimodule condition in this setting, each ϕ_g preserves the homogeneous components. However, we will use an equivalent, but different description of this comodule structure. As we discussed already in Paragraph 1.4, every left H -comodule structure leads to a right module structure over H^* . Since the character group $\hat{G} := \text{Hom}(G, K^\times)$ of group homomorphisms from G to K^\times becomes a basis of H^* if we extend group homomorphisms $\gamma : G \rightarrow K^\times$ linearly to all of H , we can consider H^* as the group ring $K[\hat{G}]$ of the character group. This means that we also have a representation

$$\hat{G} \rightarrow \text{Aut}(V), \gamma \mapsto \psi_\gamma$$

of \hat{G} . Because \hat{G} is abelian, the fact that this representation is derived from a right H^* -module structure, and not from a left H^* -module structure, does not pose a problem. Explicitly, ψ_γ is then given by the formula $\psi_\gamma(v) = \gamma(v^{(1)})v^{(2)}$. The Yetter-Drinfel'd condition implies that these two actions commute, i.e., that we have $\psi_\gamma \circ \phi_g = \phi_g \circ \psi_\gamma$ for all $g \in G$ and all $\gamma \in \hat{G}$, because ϕ_g preserves the homogeneous components.

Since we have just explained that an H -comodule structure is the same as a representation of \hat{G} , it must be possible to compute the coaction from this representation. This is achieved by the following formula:

Proposition For all $v \in V$, we have

$$\delta(v) = \frac{1}{|G|} \sum_{\gamma \in \hat{G}} \sum_{g \in G} \gamma(g^{-1}) g \otimes \psi_\gamma(v)$$

If W is a second Yetter-Drinfel'd module and the corresponding representations for W are also denoted by ϕ and ψ , the quasisymmetry and its inverse have the form

$$\begin{aligned} \sigma_{V,W}(v \otimes w) &= \frac{1}{|G|} \sum_{\gamma \in \hat{G}} \sum_{g \in G} \gamma(g^{-1}) \phi_g(w) \otimes \psi_\gamma(v) \\ \sigma_{V,W}^{-1}(w \otimes v) &= \frac{1}{|G|} \sum_{\gamma \in \hat{G}} \sum_{g \in G} \gamma(g) \psi_\gamma(v) \otimes \phi_g(w) \end{aligned}$$

Proof. The orthogonality relations for finite abelian groups assert that

$$\sum_{g \in G} \gamma(g^{-1}) \gamma'(g) = |G| \delta_{\gamma, \gamma'}$$

for all $\gamma, \gamma' \in \hat{G}$. Therefore, applying $\gamma' \otimes \text{id}_V$ to the right-hand side of the first assertion about the form of $\delta(v)$ yields

$$\begin{aligned} (\gamma' \otimes \text{id}_V) \left(\frac{1}{|G|} \sum_{\gamma \in \hat{G}} \sum_{g \in G} \gamma(g^{-1}) g \otimes \psi_\gamma(v) \right) &= \frac{1}{|G|} \sum_{\gamma \in \hat{G}} \sum_{g \in G} \gamma(g^{-1}) \gamma'(g) \psi_\gamma(v) \\ &= \sum_{\gamma \in \hat{G}} \delta_{\gamma, \gamma'} \psi_\gamma(v) = \psi_{\gamma'}(v) = \gamma'(v^{(1)}) v^{(2)} = (\gamma' \otimes \text{id}_V)(\delta(v)) \end{aligned}$$

Because the set of all $\gamma' \in \hat{G}$ is a basis of H^* , this proves the first assertion about the form of $\delta(v)$. The second assertion follows directly by inserting the first assertion into the form of the quasisymmetry and its inverse stated in Paragraph 1.1. \square

As we discussed in Paragraph 1.2, right Yetter-Drinfel'd modules are just left Yetter-Drinfel'd modules over $H^{\text{op cop}}$. Therefore, the corresponding formula for the coaction reads

$$\delta(v) = \frac{1}{|G|} \sum_{\gamma \in \hat{G}} \sum_{g \in G} \gamma(g^{-1}) \psi_\gamma(v) \otimes g$$

where ψ_γ is analogously given as $\psi_\gamma(v) = v^{(1)} \gamma(v^{(2)})$.

The proposition above has the following consequence:

Corollary For $v \in V$ and $Q \subset \hat{G}$, the following two conditions are equivalent:

1. $\psi_\gamma(v) = v$ for all $\gamma \in Q$
2. $\delta(v) \in K[Q^\perp] \otimes V$

In this case, the coaction has the form

$$\delta(v) = \frac{1}{|G|} \sum_{\gamma \in \hat{G}} \sum_{g \in Q^\perp} \gamma(g^{-1}) g \otimes \psi_\gamma(v)$$

Proof. The first assertion of the preceding proposition can be written in the form

$$\delta(v) = \frac{1}{|G|} \sum_{g \in G} g \otimes \left(\sum_{\gamma \in \hat{G}} \gamma(g^{-1}) \psi_\gamma(v) \right)$$

which shows that the homogeneous component of degree g of v is given by the formula $\frac{1}{|G|} \sum_{\gamma \in \hat{G}} \gamma(g^{-1}) \psi_\gamma(v)$. To see that the first condition implies the second, we have to show that this component vanishes if $g \notin Q^\perp$. But then there exists $\gamma' \in Q$ with $\gamma'(g) \neq 1$. As we have

$$\begin{aligned} \sum_{\gamma \in \hat{G}} \gamma(g^{-1}) \psi_\gamma(v) &= \sum_{\gamma \in \hat{G}} \gamma(g^{-1}) \psi_\gamma(\psi_{\gamma'}(v)) \\ &= \sum_{\gamma \in \hat{G}} (\gamma \gamma'^{-1})(g^{-1}) \psi_\gamma(v) = \gamma'(g) \sum_{\gamma \in \hat{G}} \gamma(g^{-1}) \psi_\gamma(v) \end{aligned}$$

this yields that $\sum_{\gamma \in \hat{G}} \gamma(g^{-1}) \psi_\gamma(v) = 0$, as asserted. To see that the second condition implies the first, we observe that for $\gamma \in Q$ and $g \in Q^\perp$, we have $\gamma(g) = 1 = \varepsilon_H(g)$, so that $\delta(v) \in K[Q^\perp] \otimes V$ entails

$$\psi_\gamma(v) = \gamma(v^{(1)}) v^{(2)} = \varepsilon_H(v^{(1)}) v^{(2)} = v$$

as asserted. \square

Although we have not assumed in this corollary that Q is a subgroup of \hat{G} , this point is not decisive, because v is stabilized by Q if and only if it is stabilized by the subgroup generated by Q .

As in the case of the proposition above, there is a version of this corollary for a right Yetter-Drinfel'd module V , which states in particular that

$$\delta(v) = \frac{1}{|G|} \sum_{\gamma \in \hat{G}} \sum_{g \in Q^\perp} \gamma(g^{-1}) \psi_\gamma(v) \otimes g$$

if $v \in V$ satisfies $\psi_\gamma(v) = v$ for all $\gamma \in Q$.

For two left Yetter-Drinfel'd modules V and W and a subgroup $Q \subset \hat{G}$ that stabilizes an element $v \in V$, we can clearly insert the form of the coaction obtained in the preceding corollary into the formula for the quasisymmetry. However, we can do more and also take an analogous subgroup of G into account:

Lemma If we assume that elements $v \in V$ and $w \in W$ are stabilized by subgroups $T \subset G$ and $Q \subset \hat{G}$ in the sense that $\psi_\gamma(v) = v$ for all $\gamma \in Q$ and $\phi_g(w) = w$ for all $g \in T$, we have

$$\begin{aligned} \sigma_{V,W}(v \otimes w) &= \frac{1}{|Q^\perp||Q \cap T^\perp|} \sum_{\gamma \in T^\perp} \sum_{g \in Q^\perp} \gamma(g^{-1}) \phi_g(w) \otimes \psi_\gamma(v) \\ \sigma_{V,W}^{-1}(w \otimes v) &= \frac{1}{|Q^\perp||Q \cap T^\perp|} \sum_{\gamma \in T^\perp} \sum_{g \in Q^\perp} \gamma(g) \psi_\gamma(v) \otimes \phi_g(w) \end{aligned}$$

Proof. By the preceding corollary, we have

$$\delta(v) = \frac{1}{|G|} \sum_{\gamma \in \hat{G}} \sum_{g \in Q^\perp} \gamma(g^{-1}) g \otimes \psi_\gamma(v)$$

As in the proof of the preceding proposition, we insert this formula into the equations for the quasisymmetry and its inverse to get

$$\begin{aligned} \sigma_{V,W}(v \otimes w) &= \frac{1}{|G|} \sum_{\gamma \in \hat{G}} \sum_{g \in Q^\perp} \gamma(g^{-1}) \phi_g(w) \otimes \psi_\gamma(v) \\ \sigma_{V,W}^{-1}(w \otimes v) &= \frac{1}{|G|} \sum_{\gamma \in \hat{G}} \sum_{g \in Q^\perp} \gamma(g) \psi_\gamma(v) \otimes \phi_g(w) \end{aligned}$$

Now suppose that $\gamma \notin QT^\perp = (Q^\perp \cap T)^\perp$. Then there exists $h \in Q^\perp \cap T$ such that $\gamma(h) \neq 1$, and since

$$\sum_{g \in Q^\perp} \gamma(g) \phi_g(w) = \sum_{g \in Q^\perp} \gamma(gh) \phi_g(\phi_h(w)) = \gamma(h) \sum_{g \in Q^\perp} \gamma(g) \phi_g(w)$$

we must have $\sum_{g \in Q^\perp} \gamma(g) \phi_g(w) = 0$. Applying this argument to γ^{-1} instead of γ , we also get that $\sum_{g \in Q^\perp} \gamma(g^{-1}) \phi_g(w) = 0$. The formulas above therefore reduce to

$$\begin{aligned} \sigma_{V,W}(v \otimes w) &= \frac{1}{|G|} \sum_{\gamma \in QT^\perp} \sum_{g \in Q^\perp} \gamma(g^{-1}) \phi_g(w) \otimes \psi_\gamma(v) \\ \sigma_{V,W}^{-1}(w \otimes v) &= \frac{1}{|G|} \sum_{\gamma \in QT^\perp} \sum_{g \in Q^\perp} \gamma(g) \psi_\gamma(v) \otimes \phi_g(w) \end{aligned}$$

Now the map $T^\perp \times Q \rightarrow QT^\perp$, $(\gamma, \gamma') \mapsto \gamma\gamma'$ is a surjective group homomorphism whose kernel consists of the pairs (γ, γ^{-1}) with $\gamma \in Q \cap T^\perp$. We can therefore write the formula for the quasisymmetry in the form

$$\begin{aligned} \sigma_{V,W}(v \otimes w) &= \frac{1}{|G||Q \cap T^\perp|} \sum_{\gamma \in T^\perp} \sum_{\gamma' \in Q} \sum_{g \in Q^\perp} (\gamma\gamma')(g^{-1}) \phi_g(w) \otimes \psi_{\gamma\gamma'}(v) \\ &= \frac{|Q|}{|G||Q \cap T^\perp|} \sum_{\gamma \in T^\perp} \sum_{g \in Q^\perp} \gamma(g^{-1}) \phi_g(w) \otimes \psi_\gamma(v) \end{aligned}$$

Since the formula for $\sigma_{V,W}^{-1}(w \otimes v)$ can be rewritten in the same way, this proves the assertion, as we have $|G| = |Q||Q^\perp|$. \square

The coefficient $|Q^\perp||Q \cap T^\perp|$ that appears in the equations stated in this lemma seems to be asymmetric in T and Q . However, as we will discuss after Lemma 2.2, this is indeed not the case.

In the case of two right Yetter-Drinfel'd modules V and W and elements $v \in V$ and $w \in W$ that are stabilized by subgroups $T \subset G$ and $Q \subset \hat{G}$ in the sense that $\phi_g(v) = v$ for all $g \in T$ and $\psi_\gamma(w) = w$ for all $\gamma \in Q$, where ϕ_g now denotes the right action of g , the corresponding formulas read

$$\begin{aligned}\sigma_{V,W}(v \otimes w) &= \frac{1}{|Q^\perp||Q \cap T^\perp|} \sum_{\gamma \in T^\perp} \sum_{g \in Q^\perp} \gamma(g^{-1}) \psi_\gamma(w) \otimes \phi_g(v) \\ \sigma_{V,W}^{-1}(w \otimes v) &= \frac{1}{|Q^\perp||Q \cap T^\perp|} \sum_{\gamma \in T^\perp} \sum_{g \in Q^\perp} \gamma(g) \phi_g(v) \otimes \psi_\gamma(w)\end{aligned}$$

These equations follow from the preceding lemma by considering right Yetter-Drinfel'd modules as left Yetter-Drinfel'd modules over $H^{\text{op cop}}$, keeping in mind that we then have to reverse the order of the tensor factors, as explained in Paragraph 1.2. Alternatively, one can of course also adapt the above proof directly to this situation, using the formula for the right coaction of H given after the preceding corollary.

It is important to note that the situation is entirely symmetric in ϕ_g and ψ_γ : As we have seen in Paragraph 1.4, we can view a left Yetter-Drinfel'd module V as a right Yetter-Drinfel'd module over $H^* \cong K[\hat{G}]$. Our discussion at the beginning of this paragraph already shows that the representation of \hat{G} that is analogous to the representation $g \mapsto \phi_g$ of G in this setup is exactly $\gamma \mapsto \psi_\gamma$. But the compatibility conditions in Paragraph 1.4 also show that the H^* -coaction, when turned into an action of $H^{**} \cong H$ and then into a representation of G , leads exactly to the representation $g \mapsto \phi_g$. Under this operation, the roles of the groups T and Q are reversed. In view of the symmetry property of the coefficient that we have already mentioned and will establish after Lemma 2.2, the formulas for the quasisymmetry and its inverse in the case of right Yetter-Drinfel'd modules therefore also arise from the corresponding formulas in the case of left Yetter-Drinfel'd modules given in the preceding lemma by interchanging ϕ_g and ψ_γ .

2.2 We now turn our attention from Yetter-Drinfel'd modules to Yetter-Drinfel'd Hopf algebras, still over the group ring of our finite abelian group G . So, we consider now a left Yetter-Drinfel'd Hopf algebra A over $H = K[G]$ and suppose that $T \subset G$ and $Q \subset \hat{G}$ are subgroups that act trivially on A , so that we have $\phi_g = \psi_\gamma = \text{id}_A$ for all $g \in T$ and all $\gamma \in Q$. We define the group

$$G' := Q^\perp / (T \cap Q^\perp)$$

Its character group can be described as follows:

Lemma $\hat{G}' \cong T^\perp / (Q \cap T^\perp)$

Proof. Every character $\gamma \in T^\perp$ induces a character

$$G' \rightarrow K^\times, \bar{g} \mapsto \gamma(g)$$

so that we get a group homomorphism from T^\perp to \hat{G}' whose kernel is $Q \cap T^\perp$. Factoring over the kernel, we get an injective homomorphism from $T^\perp/(Q \cap T^\perp)$ to \hat{G}' . This shows that $|T^\perp/(Q \cap T^\perp)| \leq |\hat{G}'|$, and it also shows that this map will be an isomorphism if $|\hat{G}'| = |T^\perp/(Q \cap T^\perp)|$.

Now every $g \in Q^\perp$ also induces a character

$$T^\perp/(Q \cap T^\perp) \rightarrow K^\times, \bar{\gamma} \mapsto \gamma(g)$$

so that we get a group homomorphism from Q^\perp to the character group of $T^\perp/(Q \cap T^\perp)$ whose kernel is $T \cap Q^\perp$. Factoring over the kernel, we get an injective homomorphism from $G' = Q^\perp/(T \cap Q^\perp)$ to the character group of $T^\perp/(Q \cap T^\perp)$, which shows that $|\hat{G}'| = |G'| \leq |T^\perp/(Q \cap T^\perp)|$. \square

We note that this lemma implies that

$$|Q^\perp|/|T \cap Q^\perp| = |G'| = |\hat{G}'| = |T^\perp|/|Q \cap T^\perp|$$

so that $|Q^\perp||Q \cap T^\perp| = |T^\perp||T \cap Q^\perp|$, which means that the coefficient appearing in Lemma 2.1 is indeed symmetric in T and Q , as we claimed there.

Clearly, the action of G on A can be restricted to Q^\perp , and this action factors over G' , so that A becomes a left $K[G']$ -module. Similarly, the action of \hat{G} on A can be restricted to T^\perp , and this action factors over $T^\perp/(Q \cap T^\perp)$, which in view of the preceding lemma yields an action of \hat{G}' on A . This action can then again be used to introduce a left $K[G']$ -comodule structure on A , which by Proposition 2.1 has the explicit form

$$\delta(a) = \frac{1}{|G'|} \sum_{\gamma \in \hat{G}'} \sum_{g \in G'} \gamma(g^{-1}) g \otimes \psi_\gamma(a)$$

As it turns out, these structures fit together:

Proposition A is a Yetter-Drinfel'd Hopf algebra over $K[G']$.

Proof. The fact that the two actions commute means that the Yetter-Drinfel'd compatibility condition is satisfied. Furthermore, both G' and \hat{G}' act by algebra and coalgebra homomorphisms, so that A is a Yetter-Drinfel'd algebra and a Yetter-Drinfel'd coalgebra over $K[G']$. The antipode S_A is also linear and colinear over $K[G']$ and still satisfies the antipode axioms. To establish the assertion, it therefore remains to show that the quasisymmetry that comes from the $K[G']$ -structure, which we denote by $\sigma'_{A,A}$, coincides with the quasisymmetry $\sigma_{A,A}$ that comes from the $K[G]$ -structure. As we just saw, the coaction is

given by

$$\begin{aligned}
\delta(a) &= \frac{1}{|G'|} \sum_{\gamma \in G'} \sum_{g \in G'} \gamma(g^{-1}) g \otimes \psi_\gamma(a) \\
&= \frac{|T \cap Q^\perp|}{|Q^\perp|} \sum_{\bar{\gamma} \in T^\perp / (Q \cap T^\perp)} \sum_{\bar{g} \in Q^\perp / (T \cap Q^\perp)} \gamma(g^{-1}) \bar{g} \otimes \psi_{\bar{\gamma}}(a) \\
&= \frac{1}{|Q^\perp|} \sum_{\bar{\gamma} \in T^\perp / (Q \cap T^\perp)} \sum_{g \in Q^\perp} \gamma(g^{-1}) \bar{g} \otimes \psi_{\bar{\gamma}}(a) \\
&= \frac{1}{|Q^\perp||Q \cap T^\perp|} \sum_{\gamma \in T^\perp} \sum_{g \in Q^\perp} \gamma(g^{-1}) \bar{g} \otimes \psi_\gamma(a)
\end{aligned}$$

Using Heyneman-Sweedler notation with respect to the $K[G']$ -structure, we find the expression

$$\sigma'_{A,A}(a \otimes b) = (a^{(1)}.b) \otimes a^{(2)} = \frac{1}{|Q^\perp||Q \cap T^\perp|} \sum_{\gamma \in T^\perp} \sum_{g \in Q^\perp} \gamma(g^{-1}) \phi_g(b) \otimes \psi_\gamma(a)$$

for the quasisymmetry. It therefore follows from Lemma 2.1 that

$$\sigma'_{A,A}(a \otimes b) = \sigma_{A,A}(a \otimes b)$$

for all $a, b \in A$. This implies that the algebra structure determined by $\sigma'_{A,A}$ on the second tensor power of A coincides with the algebra structure of $A \hat{\otimes} A$, which is what we needed to show. \square

3 The Commutative Case

3.1 In this section, we turn to the main object of our study: We consider a commutative semisimple left Yetter-Drinfel'd Hopf algebra A over the group ring $H = K[G]$ of a finite abelian group G . As in Section 2, the base field K is assumed to be algebraically closed of characteristic zero, except for a minor comment in Paragraph 3.9. Then A is finite-dimensional by Proposition 1.5, and because K is algebraically closed, semisimplicity implies that A has a basis consisting of primitive idempotents, any two of which are orthogonal. The set of all primitive idempotents of A will be denoted by E . Since the mappings ϕ_g and ψ_γ defined in Paragraph 2.1 are algebra automorphisms, they permute these primitive idempotents. The dual basis of E consists exactly of the (one-dimensional) characters, i.e., the algebra homomorphisms from A to K , and the set of all these characters is precisely the set $G(A^*)$ of all group-like elements in the dual A^* .

With each primitive idempotent, we associate a number of objects that will play an important role in the sequel:

Definition Suppose that $e \in E$ is a primitive idempotent of A .

1. The character associated with e is the unique algebra homomorphism to the base field $\eta_e : A \rightarrow K$ with the property that $\eta_e(e) = 1$ and $\eta_e(e') = 0$ for all primitive idempotents $e' \neq e$.
2. The inertia group of e is the group $T_e := \{g \in G \mid \phi_g(e) = e\}$.
3. The isotropy group of e is the group $Q_e := \{\gamma \in \hat{G} \mid \psi_\gamma(e) = e\}$.
4. The index group of e is the group $G_e := Q_e^\perp / (T_e \cap Q_e^\perp)$.
5. The index of e is the number $|G_e|$.
6. The orbit of e under the action of Q_e^\perp is the set $O_e := \{\phi_g(e) \mid g \in Q_e^\perp\}$.
7. The full orbit of e is the set $\hat{O}_e := \{\psi_\gamma(\phi_g(e)) \mid g \in G, \gamma \in \hat{G}\}$.
8. The stability set of e is the set $\check{O}_e := \{e' \in E \mid T_e \subset T_{e'} \text{ and } Q_e \subset Q_{e'}\}$.

The ideals spanned by these sets will be denoted by

$$I_e := \text{Span}(O_e) \quad \hat{I}_e := \text{Span}(\hat{O}_e) \quad \check{I}_e := \text{Span}(\check{O}_e)$$

and the unique ideals that complement them will be denoted by J_e , \hat{J}_e , and \check{J}_e , respectively. Stated differently, J_e , \hat{J}_e , and \check{J}_e are spanned by all primitive idempotents that are not contained in O_e , \hat{O}_e , and \check{O}_e , respectively, and they satisfy $A = I_e \oplus J_e = \hat{I}_e \oplus \hat{J}_e = \check{I}_e \oplus \check{J}_e$. The characters that correspond to these sets of idempotents will be denoted by

$$U_e := \{\eta_{e'} \mid e' \in O_e\} \quad \hat{U}_e := \{\eta_{e'} \mid e' \in \hat{O}_e\} \quad \check{U}_e := \{\eta_{e'} \mid e' \in \check{O}_e\}$$

so that

$$J_e^\perp = \text{Span}(U_e) \quad \hat{J}_e^\perp = \text{Span}(\hat{U}_e) \quad \check{J}_e^\perp = \text{Span}(\check{U}_e)$$

By construction, we have $O_e \subset \hat{O}_e \subset \check{O}_e$ and therefore

$$I_e \subset \hat{I}_e \subset \check{I}_e \quad J_e \supset \hat{J}_e \supset \check{J}_e \quad U_e \subset \hat{U}_e \subset \check{U}_e$$

It follows directly from these definitions that \hat{O}_e and \check{O}_e , and accordingly also \hat{I}_e , \check{I}_e , \hat{J}_e , \check{J}_e , \hat{U}_e , and \check{U}_e , are stable under both G and \hat{G} . Also by construction we have $\dim(I_e) = |O_e| = |G_e|$. We will furthermore speak of the index of the character η_e , which is by definition the index of the corresponding primitive idempotent e . These definitions should be compared with [30], Def. 2.3, p. 27.

We can compute a primitive idempotent from its character via the integrals introduced in Paragraph 1.5:

Proposition If $e \in E$ is a primitive idempotent, we have

$$\begin{aligned} e &= \eta_e^{-1}(\Lambda_{A(1)})\Lambda_{A(2)} = \eta_e(\Lambda_{A(1)})S_A(\Lambda_{A(2)}) \\ &= \Lambda_{A(1)}\eta_e^{-1}(\Lambda_{A(2)}) = S_A(\Lambda_{A(1)})\eta_e(\Lambda_{A(2)}) \end{aligned}$$

Furthermore, we have $\lambda_A(e) = 1$.

Proof. We know from Proposition 1.5 that

$$e = \lambda_A(e\Lambda_{A(1)})S_A(\Lambda_{A(2)}) = \lambda_A(e)\eta_e(\Lambda_{A(1)})S_A(\Lambda_{A(2)})$$

and also $e = S_A(\Lambda_{A(1)})\eta_e(\Lambda_{A(2)})\lambda_A(e)$. If we apply η_e to the first equation, we get that

$$1 = \eta_e(e) = \lambda_A(e)\eta_e(\Lambda_{A(1)})\eta_e(S_A(\Lambda_{A(2)})) = \lambda_A(e)\varepsilon_A(\Lambda_A)\eta_e(1_A) = \lambda_A(e)$$

Inserting this back into these equations, we get two of the four forms of e . The remaining two follow by substituting the other form of the Casimir element into the ones already established, as we have $\eta_e^{-1} = \eta_e \circ S_A$. \square

The fact that $\lambda_A(e) = 1$ gives another proof for the assertion that λ_A is the character of the regular representation made in Proposition 1.5, since the character of the regular representation clearly also takes the value 1 on primitive idempotents, and the primitive idempotents form a basis, as discussed at the beginning of this paragraph.

Let us note a remarkable consequence of this proposition:

Corollary For primitive idempotents e and e' , we have $\eta_e^{-1}(e') = \eta_{e'}^{-1}(e)$.

Proof. We have seen in the last proposition that

$$e = \eta_e^{-1}(\Lambda_{A(1)})\Lambda_{A(2)} = \Lambda_{A(1)}\eta_e^{-1}(\Lambda_{A(2)})$$

which obviously implies that

$$\eta_{e'}^{-1}(e) = \eta_e^{-1}(\Lambda_{A(1)})\eta_{e'}^{-1}(\Lambda_{A(2)}) = \eta_{e'}^{-1}(\Lambda_{A(1)})\eta_e^{-1}(\Lambda_{A(2)})$$

If we interchange e and e' in this equation, it becomes

$$\eta_e^{-1}(e') = \eta_{e'}^{-1}(\Lambda_{A(1)})\eta_e^{-1}(\Lambda_{A(2)}) = \eta_e^{-1}(\Lambda_{A(1)})\eta_{e'}^{-1}(\Lambda_{A(2)})$$

The assertion then follows by comparing these two equations. \square

We note that the proof of this corollary shows again that Λ_A is cocommutative, as we already stated in Proposition 1.5: We have just seen in this proof that

$$(\eta_e^{-1} \otimes \eta_{e'}^{-1})(\Lambda_{A(1)} \otimes \Lambda_{A(2)}) = (\eta_e^{-1} \otimes \eta_{e'}^{-1})(\Lambda_{A(2)} \otimes \Lambda_{A(1)})$$

Since the tensors $\eta_e^{-1} \otimes \eta_{e'}^{-1}$ form a basis of $A^* \otimes A^*$, this implies that we have $\Lambda_{A(1)} \otimes \Lambda_{A(2)} = \Lambda_{A(2)} \otimes \Lambda_{A(1)}$.

3.2 We now investigate the ideal structure of the algebra $A \hat{\otimes} A$ introduced in Paragraph 1.3 in our situation. For this, we need to associate with two primitive idempotents e and e' two ideals which are defined in a similar way to the ideals I_e and $I_{e'}$, but take the interaction of e and e' into account. So, we consider the orbits

$$O := \{\phi_g(e) \mid g \in Q_{e'}^\perp\} \quad O' := \{\psi_\gamma(e') \mid \gamma \in T_e^\perp\}$$

and denote the ideals that they span by $I := \text{Span}(O)$ and $I' := \text{Span}(O')$, respectively. Inside these ideals, we need to consider certain elements which arise from the idempotents by a discrete Fourier transform:

Definition

1. For every $\gamma \in \hat{G}$, we define

$$w_\gamma := \frac{1}{|T_e \cap Q_{e'}^\perp|} \sum_{g \in Q_{e'}^\perp} \gamma(g^{-1}) \phi_g(e) \in I$$

2. For every $g \in G$, we define

$$u_g := \frac{1}{|Q_{e'} \cap T_e^\perp|} \sum_{\gamma \in T_e^\perp} \gamma(g^{-1}) \psi_\gamma(e') \in I'$$

We record that in the case where $\gamma = \varepsilon_H$ is the counit, w_γ is just the sum of all elements of O , which we denote by e_I (cf. [30], Par. 6.6, p. 96). If we consider the ideal I as a non-unital subalgebra of A , then e_I is the unit element of this algebra.

The following lemma lists the basic properties of the elements w_γ :

Lemma

1. O and O' have the same cardinality m .
2. For all $g \in Q_{e'}^\perp$, we have $\phi_g(w_\gamma) = \gamma(g) w_\gamma$.
3. If γ and γ' belong to the same coset in $\hat{G}/Q_{e'}$, we have $w_\gamma = w_{\gamma'}$.
4. If $\gamma \notin T_e^\perp Q_{e'}$, we have $w_\gamma = 0$.
5. If $\gamma \in T_e^\perp Q_{e'}$, we have $\eta_e(w_\gamma) = 1$.
6. If $g_1, \dots, g_m \in Q_{e'}^\perp$ is a system of representatives for the cosets in the quotient $Q_{e'}^\perp / (T_e \cap Q_{e'}^\perp)$, then we have

$$w_\gamma = \sum_{i=1}^m \gamma(g_i^{-1}) \phi_{g_i}(e)$$

for all $\gamma \in T_e^\perp Q_{e'}$.

7. If $\gamma_1, \dots, \gamma_m \in T_e^\perp$ is a system of representatives for the cosets in the quotient $T_e^\perp/(Q_{e'} \cap T_e^\perp)$, then the elements $w_{\gamma_1}, \dots, w_{\gamma_m}$ form a basis of I .

8. For $g \in Q_{e'}^\perp$, we then have

$$\phi_g(e) = \frac{1}{m} \sum_{j=1}^m \gamma_j(g) w_{\gamma_j}$$

Proof. (1) We have $|O| = |Q_{e'}^\perp/(T_e \cap Q_{e'}^\perp)|$ and $|O'| = |T_e^\perp/(Q_{e'} \cap T_e^\perp)|$. Since we have seen in the proof of Lemma 2.2 that the cardinalities of these two factor groups are equal, the first assertion holds.

(2) The second and the third assertion follow more or less directly from the definition. For the fourth assertion, we note that if $\gamma \notin T_e^\perp Q_{e'} = (T_e \cap Q_{e'}^\perp)^\perp$, we can find $g \in T_e \cap Q_{e'}^\perp$ satisfying $\gamma(g) \neq 1$, which implies that

$$w_\gamma = \phi_g(w_\gamma) = \gamma(g) w_\gamma$$

by the second property, so that $w_\gamma = 0$.

(3) The fifth assertion holds since

$$\begin{aligned} \eta_e(w_\gamma) &= \frac{1}{|T_e \cap Q_{e'}^\perp|} \sum_{g \in Q_{e'}^\perp} \gamma(g^{-1}) \eta_e(\phi_g(e)) \\ &= \frac{1}{|T_e \cap Q_{e'}^\perp|} \sum_{g \in T_e \cap Q_{e'}^\perp} \gamma(g^{-1}) \eta_e(e) = 1 \end{aligned}$$

where we have used in the last step that $\gamma(g) = 1$ if $g \in T_e \cap Q_{e'}^\perp$ and $\gamma \in T_e^\perp Q_{e'}$.

(4) To prove the sixth property, we use the system of representatives to write the definition of w_γ in the form

$$w_\gamma = \frac{1}{|T_e \cap Q_{e'}^\perp|} \sum_{i=1}^m \sum_{g \in T_e \cap Q_{e'}^\perp} \gamma(g^{-1} g_i^{-1}) \phi_{g_i g}(e)$$

As in the previous step, we have for $g \in T_e \cap Q_{e'}^\perp$ and $\gamma \in T_e^\perp Q_{e'}$ that $\phi_g(e) = e$ and $\gamma(g^{-1}) = 1$. Therefore, the summation over g can be carried out, which gives the assertion.

(5) For the seventh property, we have that $O = \{\phi_{g_1}(e), \dots, \phi_{g_m}(e)\}$ is a basis of I by definition, and the base change

$$w_{\gamma_j} = \sum_{i=1}^m \gamma_j(g_i^{-1}) \phi_{g_i}(e)$$

is given by an invertible matrix, as we saw in the proof of Lemma 2.2. By the orthogonality relations for finite abelian groups, which we have already recalled in Paragraph 2.1, the inverse of this matrix is $(\gamma_j(g_i)/m)$, so that we get

$$\phi_{g_i}(e) = \frac{1}{m} \sum_{j=1}^m \gamma_j(g_i) w_{\gamma_j}$$

If $i \leq m$ is chosen so that g and g_i are in the same coset of the quotient $Q_{e'}^\perp/(T_e \cap Q_{e'}^\perp)$, we can replace g_i by g on the left-hand and the right-hand side to get the last assertion. \square

It follows from the discussion in Paragraph 1.4 together with Lemma 1.3 that we can consider $A^{\text{op cop}} = A^{\text{cop}}$ as a left Yetter-Drinfel'd Hopf algebra over the dual Hopf algebra $H^* = H^{*\text{op cop}} \cong K[\hat{G}]$. As we have explained at the end of Paragraph 2.1, the roles of ϕ_g and ψ_γ are interchanged from this viewpoint. If we also interchange the idempotents e and e' , then the elements w_γ turn into the elements u_g . In this way, the following properties of the elements u_g follow directly from the corresponding properties of the elements w_γ :

Corollary

1. For all $\gamma \in T_e^\perp$, we have $\psi_\gamma(u_g) = \gamma(g)u_g$.
2. If g and g' belong to the same coset in G/T_e , we have $u_g = u_{g'}$.
3. If $g \notin Q_{e'}^\perp T_e$, we have $u_g = 0$.
4. If $g \in Q_{e'}^\perp T_e$, we have $\eta_{e'}(u_g) = 1$.
5. If $\gamma_1, \dots, \gamma_m \in T_e^\perp$ is a system of representatives for the cosets in the quotient $T_e^\perp/(Q_{e'} \cap T_e^\perp)$, then we have

$$u_g = \sum_{j=1}^m \gamma_j(g^{-1}) \psi_{\gamma_j}(e')$$

for all $g \in Q_{e'}^\perp T_e$.

6. If $g_1, \dots, g_m \in Q_{e'}^\perp$ is a system of representatives for the cosets in the quotient $Q_{e'}^\perp/(T_e \cap Q_{e'}^\perp)$, then the elements u_{g_1}, \dots, u_{g_m} form a basis of I' .
7. For $\gamma \in T_e^\perp$, we then have

$$\psi_\gamma(e') = \frac{1}{m} \sum_{i=1}^m \gamma(g_i) u_{g_i}$$

As in [30], Prop. 6.5, p. 94, we can use these elements to describe the ideal structure of the algebra $A \hat{\otimes} A$ introduced in Paragraph 1.3:

Proposition

1. For all $a \in A$, we have $a^{(1)}\eta_{e'}(a^{(2)}) \in K[Q_{e'}^\perp]$.
2. For all $a \in I$ and all $g \in G$, we have $(u_g^{(1)}.a) \otimes u_g^{(2)} = \phi_g(a) \otimes u_g$.
3. $I \hat{\otimes} Ke'$ is a minimal left ideal of $A \hat{\otimes} A$.
4. A is an $A \hat{\otimes} A$ -module with respect to the module structure

$$(a \otimes a').b = a(a'^{(1)}.b)\eta_{e'}(a'^{(2)})$$

5. For this module structure, I is a simple $A \hat{\otimes} A$ -submodule of A .

6. $I \hat{\otimes} I'$ is a minimal two-sided ideal of $A \hat{\otimes} A$.

Proof. (1) The ideal $\hat{I}_{e'}$ and its complement $\hat{J}_{e'}$ are invariant under \hat{G} and therefore are H^* -submodules, i.e., H -subcomodules. If $a \in \hat{I}_{e'}$, we obtain from Corollary 2.1 that $\delta(a) \in K[Q_{e'}^\perp] \otimes A$ and therefore $a^{(1)}\eta_{e'}(a^{(2)}) \in K[Q_{e'}^\perp]$. On the other hand, if $a \in \hat{J}_{e'}$, then we have that $\delta(a) \in H \otimes \hat{J}_{e'}$ and therefore $a^{(1)}\eta_{e'}(a^{(2)}) = 0 \in K[Q_{e'}^\perp]$.

(2) To prove the second assertion, we can assume that $a = w_\gamma$ for some $\gamma \in T_e^\perp$, because these elements span I by the preceding lemma. If $g \notin Q_{e'}^\perp T_e$, we have $u_g = 0$ by the preceding corollary, so that the assertion is correct. If $g \in Q_{e'}^\perp T_e$, we also know from the preceding corollary that we can modify g so that $g \in Q_{e'}^\perp$, and the right-hand side also does not change under this modification. Since we know from Corollary 2.1 that $\delta(u_g) \in K[Q_{e'}^\perp] \otimes A$, it follows from the preceding lemma that

$$\begin{aligned} (u_g^{(1)}.w_\gamma) \otimes u_g^{(2)} &= \gamma(u_g^{(1)})w_\gamma \otimes u_g^{(2)} = w_\gamma \otimes \psi_\gamma(u_g) \\ &= w_\gamma \otimes \gamma(g)u_g = \gamma(g)w_\gamma \otimes u_g = \phi_g(w_\gamma) \otimes u_g \end{aligned}$$

establishing our claim.

- (3) Now to see that $I \hat{\otimes} Ke'$ is a left ideal, we observe that for $b \in I$ we have

$$(a \otimes a')(b \otimes e') = a(a'^{(1)}.b) \otimes a'^{(2)}e' = a(a'^{(1)}.b)\eta_{e'}(a'^{(2)}) \otimes e'$$

and $(a'^{(1)}.b)\eta_{e'}(a'^{(2)}) \in I$ by the first assertion. The minimality will be discussed in the sixth step below.

(4) The fourth assertion can be proved directly by verifying the module axioms. However, we give a different proof with the help of an induced module construction: We can view A as a subalgebra of $A \hat{\otimes} A$ by mapping a to $1_A \otimes a$. Turning the base field K into an A -module by using $\eta_{e'}$, we can then form the

induced module $(A \hat{\otimes} A) \otimes_A K$, which is isomorphic to A as a vector space via $b \mapsto (b \otimes 1_A) \otimes_A 1$. Now we have

$$\begin{aligned}(a \otimes a').((b \otimes 1_A) \otimes_A 1) &= (a(a'^{(1)}.b) \otimes a'^{(2)}) \otimes_A 1 \\ &= (a(a'^{(1)}.b) \otimes 1_A) \otimes_A a'^{(2)}.1 = (a(a'^{(1)}.b)\eta_{e'}(a'^{(2)})) \otimes 1_A \otimes_A 1\end{aligned}$$

If we use the isomorphism above to transfer this module structure to A , we get the module structure that appears in the fourth assertion.

(5) The fact that I is an $A \hat{\otimes} A$ -submodule of A with respect to this module structure follows from the first assertion. To see that I is simple, we consider a nonzero submodule U of I . Because $(a \otimes 1_A).b = ab$, U is in particular a left ideal of A and therefore spanned by a subset of the idempotents in O . By the second assertion, we have for $g \in Q_{e'}^\perp$ and $b \in I$ that

$$(1_A \otimes u_g).b = \phi_g(b)\eta_{e'}(u_g) = \phi_g(b)$$

where we have used the fact that $\eta_{e'}(u_g) = 1$ established in the preceding corollary. Therefore, the set of idempotents that span U is stable under $Q_{e'}^\perp$. But since O is a $Q_{e'}^\perp$ -orbit by definition, this proves $U = I$.

(6) Of course, the left ideal $I \hat{\otimes} Ke'$ of $A \hat{\otimes} A$ is also a left $A \hat{\otimes} A$ -module by multiplication. But our computation in the third step then shows that

$$I \rightarrow I \hat{\otimes} Ke', a \mapsto a \otimes e'$$

is an isomorphism of $A \hat{\otimes} A$ -modules. Therefore, the simplicity of I implies the minimality of $I \hat{\otimes} Ke'$.

(7) To see that $I \hat{\otimes} I'$ is a left ideal, we note that

$$I \hat{\otimes} I' = \bigoplus_{\tilde{e}' \in O'} I \hat{\otimes} K \tilde{e}'$$

Since the elements of O' have the same isotropy group $Q_{e'}$ as e' , the summands in this decomposition are left ideals by the third assertion.

(8) To see that $I \hat{\otimes} I'$ is a right ideal, we have to show for $a \in I$, $a' \in I'$, and all $b, b' \in A$ that

$$(a \otimes a')(b \otimes b') = a(a'^{(1)}.b) \otimes a'^{(2)}b' \in I \hat{\otimes} I'$$

For this, we introduce the ideal J spanned by all primitive idempotents that are not in O . Then we have $A = I \oplus J$, and both I and J are invariant under $Q_{e'}^\perp$. From Corollary 2.1, we know that $\delta(a') \in K[Q_{e'}^\perp] \otimes A$. If $b \in J$, we therefore have $(a'^{(1)}.b) \otimes a'^{(2)} \in J \otimes A$, so that

$$(a \otimes a')(b \otimes b') = a(a'^{(1)}.b) \otimes a'^{(2)}b' = 0 \in I \hat{\otimes} I'$$

It remains to consider the case $b \in I$. For this, we can assume that $a' = u_g$ for some $g \in Q_{e'}^\perp$, because these elements span I' by the preceding corollary. But then we get from the second assertion that

$$(a \otimes u_g)(b \otimes b') = a(u_g^{(1)}.b) \otimes u_g^{(2)}b' = a\phi_g(b) \otimes u_gb' \in I \hat{\otimes} I'$$

as asserted.

(9) The minimality of $I \hat{\otimes} I'$ now follows from a result of W. Burnside (cf. [6], Cor. 1.16, p. 45), which, since the argument in the fifth step also shows that I is simple as an $I \hat{\otimes} I'$ -module, implies that the structure map $I \hat{\otimes} I' \rightarrow \text{End}_K(I)$ is surjective, and therefore bijective by dimension considerations. \square

It follows from this discussion that the left ideals $I \hat{\otimes} K\tilde{e}'$ for $\tilde{e}' \in O'$ that appear in the seventh step of the preceding proof are all isomorphic, because we have now seen that they are left ideals in a matrix algebra of the correct dimension. Equivalently, the $A \hat{\otimes} A$ -module structure on I considered in the fifth assertion must be isomorphic to the one that arises in the same way from the character $\eta_{\tilde{e}'}$ instead of $\eta_{e'}$. If $\tilde{e}' = \psi_\gamma(e')$ for $\gamma \in T_e^\perp$, this isomorphism is indeed just given by multiplication with $w_{\gamma^{-1}}$: Since $\eta_{\tilde{e}'} = \psi_{\gamma^{-1}}^*(\eta_{e'}) = \eta_{e'} \circ \psi_{\gamma^{-1}}$ is the character corresponding to \tilde{e}' , we have

$$\begin{aligned} (a \otimes a').(bw_{\gamma^{-1}}) &= a(a'^{(1)}.(bw_{\gamma^{-1}}))\eta_{e'}(a'^{(2)}) = a(a'^{(1)}.b)(a'^{(2)}.w_{\gamma^{-1}})\eta_{e'}(a'^{(3)}) \\ &= a(a'^{(1)}.b)(\gamma^{-1}(a'^{(2)})w_{\gamma^{-1}})\eta_{e'}(a'^{(3)}) = a(a'^{(1)}.b)w_{\gamma^{-1}}\eta_{e'}(\psi_{\gamma^{-1}}(a'^{(2)})) \\ &= a(a'^{(1)}.b)w_{\gamma^{-1}}\eta_{\tilde{e}'}(a'^{(2)}) \end{aligned}$$

where the third equality uses the fact that $a^{(1)}\eta_{e'}(a^{(2)}) \in K[Q_{e'}^\perp]$ established in the preceding proposition.

3.3 For primitive idempotents e and e' , we know from [30], Prop. 1.5.2, p. 13 that the product $\eta_e\eta_{e'}$ of the corresponding characters is again a character if η_e is H -linear or $\eta_{e'}$ is colinear. Now we want to analyze what happens in general. We use the notation introduced in the preceding paragraph:

Theorem

1. There are distinct characters $\omega_1, \dots, \omega_m$ such that

$$\eta_{\tilde{e}}\eta_{\tilde{e}'} \in \text{Span}(\omega_1, \dots, \omega_m)$$

for all $\tilde{e} \in O$ and all $\tilde{e}' \in O'$. In particular, $\eta_e\eta_{e'} \in \text{Span}(\omega_1, \dots, \omega_m)$.

2. If, for $\gamma \in T_e^\perp$, the orbit O is stable under ψ_γ , then $\{\omega_1, \dots, \omega_m\}$ is stable under ψ_γ^* .
3. If, for $g \in Q_{e'}^\perp$, the orbit O' is stable under ϕ_g , then $\{\omega_1, \dots, \omega_m\}$ is stable under ϕ_g^* .

Proof. (1) We have seen in Proposition 3.2 that I is a simple $A \hat{\otimes} A$ -submodule of A , with respect to the module structure described there. Since the coproduct $\Delta_A : A \rightarrow A \hat{\otimes} A$ is an algebra homomorphism, I also becomes an A -module by restriction along Δ_A . Since A is commutative, this A -module can be decomposed into a direct sum of one-dimensional A -modules. Therefore there is a basis v_1, \dots, v_m of I such that $a.v_k = \omega_k(a)v_k$ for characters $\omega_1, \dots, \omega_m$. Explicitly, this equation asserts that

$$\omega_k(a)v_k = a.v_k = \Delta_A(a).v_k = a_{(1)}(a_{(2)}^{(1)}.v_k)\eta_{e'}(a_{(2)}^{(2)})$$

(2) For $\gamma \in T_e^\perp$, we can write w_γ in the form

$$w_\gamma = \sum_{k=1}^m \xi_k v_k$$

since v_1, \dots, v_m is a basis of I . We then have

$$\begin{aligned} a_{(1)}w_\gamma\psi_\gamma^*(\eta_{e'})(a_{(2)}) &= a_{(1)}w_\gamma\gamma(a_{(2)}^{(1)})\eta_{e'}(a_{(2)}^{(2)}) = a_{(1)}(a_{(2)}^{(1)}.w_\gamma)\eta_{e'}(a_{(2)}^{(2)}) \\ &= \sum_{k=1}^m \xi_k a_{(1)}(a_{(2)}^{(1)}.v_k)\eta_{e'}(a_{(2)}^{(2)}) = \sum_{k=1}^m \xi_k \omega_k(a)v_k \end{aligned}$$

where we have used for the second equality again that $a^{(1)}\eta_{e'}(a^{(2)}) \in K[Q_{e'}^\perp]$ by Proposition 3.2. For $g \in Q_{e'}^\perp$, we have by Lemma 3.2 that

$$\phi_g^*(\eta_e)(w_\gamma) = \eta_e(\phi_g(w_\gamma)) = \gamma(g)\eta_e(w_\gamma) = \gamma(g)$$

Therefore we get by applying $\phi_g^*(\eta_e)$ to the equation above that

$$\begin{aligned} \gamma(g)\phi_g^*(\eta_e)(a_{(1)})\psi_\gamma^*(\eta_{e'})(a_{(2)}) &= \phi_g^*(\eta_e)(a_{(1)}w_\gamma)\psi_\gamma^*(\eta_{e'})(a_{(2)}) \\ &= \sum_{k=1}^m \xi_k \omega_k(a)\phi_g^*(\eta_e)(v_k) \end{aligned}$$

showing that

$$\phi_g^*(\eta_e)\psi_\gamma^*(\eta_{e'}) = \gamma(g^{-1}) \sum_{k=1}^m \xi_k \phi_g^*(\eta_e)(v_k)\omega_k$$

If now $\tilde{e} \in O$ and $\tilde{e}' \in O'$, we have $\tilde{e} = \phi_{g^{-1}}(e)$ for some $g \in Q_{e'}^\perp$ and similarly $\tilde{e}' = \psi_{\gamma^{-1}}(e')$ for some $\gamma \in T_e^\perp$. The corresponding characters are $\eta_{\tilde{e}} = \phi_g^*(\eta_e)$ and $\eta_{\tilde{e}'} = \psi_\gamma^*(\eta_{e'})$. Therefore the last equation shows that

$$\eta_{\tilde{e}}\eta_{\tilde{e}'} \in \text{Span}(\omega_1, \dots, \omega_m)$$

Since $\eta_{e'}$ is invertible, the elements $\eta_{\tilde{e}}\eta_{e'}$ for $\tilde{e} \in O$ are linearly independent, which implies that the characters $\omega_1, \dots, \omega_m$ must be distinct.

(3) To prove the second assertion, we argue as follows: We have

$$\text{Span}(\omega_1, \dots, \omega_m) = \text{Span}(\{\eta_{\tilde{e}}\eta_{\tilde{e}'} \mid \tilde{e} \in O, \tilde{e}' \in O'\})$$

By applying ψ_γ^* , this becomes

$$\text{Span}(\psi_\gamma^*(\omega_1), \dots, \psi_\gamma^*(\omega_m)) = \text{Span}(\{\psi_\gamma^*(\eta_{\tilde{e}})\psi_\gamma^*(\eta_{\tilde{e}'}) \mid \tilde{e} \in O, \tilde{e}' \in O'\})$$

If $\gamma \in T_e^\perp$, then O' is stable under ψ_γ anyway. Therefore, if O is stable under ψ_γ , we get

$$\text{Span}(\psi_\gamma^*(\omega_1), \dots, \psi_\gamma^*(\omega_m)) = \text{Span}(\omega_1, \dots, \omega_m)$$

which implies the assertion, since distinct group-like elements are linearly independent (cf. [19], Def. 1.3.4, p. 4; [22], Lem. 2.1.12, p. 25; [32], Prop. 3.2.1, p. 54). The proof of the third assertion is similar. \square

The preceding theorem generalizes the results in [30], Prop. 6.6, p. 95. It is worth mentioning that $\{\omega_1, \dots, \omega_m\}$ is the smallest set of characters with the property that $\eta_e\eta_{e'} \in \text{Span}(\omega_1, \dots, \omega_m)$; in other words, no coefficient in the expansion of $\eta_e\eta_{e'}$ in terms of $\omega_1, \dots, \omega_m$ vanishes. To see this, we revisit the equation

$$\phi_g^*(\eta_e)\psi_\gamma^*(\eta_{e'}) = \gamma(g^{-1}) \sum_{k=1}^m \xi_k \phi_g^*(\eta_e)(v_k) \omega_k$$

obtained in the second step of the preceding proof. In this equation, the coefficients ξ_k depend on γ , but not on g , whereas the coefficients $\phi_g^*(\eta_e)(v_k)$ clearly depend on g , but not on γ . If one of the coefficients ξ_1, \dots, ξ_m , say ξ_i , would vanish, then this equation would show that for a fixed $\gamma \in T_e^\perp$, but for all $g \in Q_{e'}^\perp$, we have

$$\phi_g^*(\eta_e)\psi_\gamma^*(\eta_{e'}) \in \text{Span}(\omega_1, \dots, \omega_{i-1}, \omega_{i+1}, \dots, \omega_m)$$

contradicting the linear independence of the elements on the left. A similar argument with the roles of g and γ reversed shows that the coefficients $\phi_g^*(\eta_e)(v_k)$ are all nonzero, so that the coefficient $\gamma(g^{-1})\xi_k \phi_g^*(\eta_e)(v_k)$ of ω_k in the above equation is nonzero. For $g = 1$ and $\gamma = \varepsilon_H$, this yields our claim.

We record the following simple consequence of the preceding theorem:

Corollary For two primitive idempotents $e, e' \in E$, the following conditions are equivalent:

1. $\eta_e\eta_{e'}$ is a character.
2. $Q_{e'}^\perp \subset T_e$
3. $\sigma_{A^*, A^*}(\eta_e \otimes \eta_{e'}) = \eta_{e'} \otimes \eta_e$

Proof. In view of the preceding discussion, the first condition is equivalent to the statement that $m = 1$. But since $m = |O|$ by Lemma 3.2, this is equivalent to the second condition.

It follows directly from the compatibility between product and coproduct discussed in Paragraph 1.3 that the third condition implies the first. Conversely, it is not difficult to reverse this argument to deduce that the first condition implies the third; a very similar argument can be found in [30], Prop. 1.1, p. 8. However, it is even easier to use the formula for the quasisymmetry given after Lemma 2.1 to show that the second condition implies the third. From the second condition, we get that also $T_e^\perp \subset Q_{e'}$, and therefore the formula for the quasisymmetry reduces to

$$\begin{aligned}\sigma_{A^*, A^*}(\eta_e \otimes \eta_{e'}) &= \frac{1}{|Q_{e'}^\perp||Q_{e'} \cap T_e^\perp|} \sum_{\gamma \in T_e^\perp} \sum_{g \in Q_{e'}^\perp} \gamma(g^{-1}) \psi_\gamma^*(\eta_{e'}) \otimes \phi_g^*(\eta_e) \\ &= \frac{1}{|Q_{e'}^\perp||T_e^\perp|} \sum_{\gamma \in T_e^\perp} \sum_{g \in Q_{e'}^\perp} \gamma(g^{-1}) \eta_{e'} \otimes \eta_e = \eta_{e'} \otimes \eta_e\end{aligned}$$

because in this situation we have $\gamma(g^{-1}) = 1$ for $\gamma \in T_e^\perp$ and $g \in Q_{e'}^\perp$. \square

3.4 As we will discuss below in greater detail, the image of an ideal under the antipode is in general not again an ideal. However, for a primitive idempotent $e \in E$, there is a minimal ideal containing e whose image under the antipode is again an ideal, namely the ideal I_e :

Theorem For a primitive idempotent $e \in E$, we have that $S_A(I_e)$ is an ideal. Conversely, if $I \subset A$ is an ideal containing e with the property that $S_A(I)$ is an ideal, then we have that $I_e \subset I$.

Proof. (1) To prove the first assertion, we use the ideal \hat{I}_e and its complement \hat{J}_e introduced in Paragraph 3.1. From the relation between antipode and product stated in Paragraph 1.3 and the formula for the inverse quasisymmetry in Proposition 2.1, we get

$$S_A(b)S_A(a) = S_A(a^{(2)}(S_H^{-1}(a^{(1)}) \cdot b)) = \frac{1}{|G|} \sum_{\gamma \in \hat{G}} \sum_{g \in G} \gamma(g) S_A(\psi_\gamma(a) \phi_g(b))$$

Suppose now that $b \in I_e$. If $a \in \hat{J}_e$, then this expression is zero, and in particular in $S_A(I_e)$. But if $a \in \hat{I}_e$, then we also have that $\psi_\gamma(a) = a$ for all $\gamma \in Q_e$ and therefore can use the formula for the inverse quasisymmetry in Lemma 2.1 instead to get

$$S_A(b)S_A(a) = \frac{1}{|Q_e^\perp||Q_e \cap T_e^\perp|} \sum_{\gamma \in T_e^\perp} \sum_{g \in Q_e^\perp} \gamma(g) S_A(\psi_\gamma(a) \phi_g(b)) \in S_A(I_e)$$

Since $A = \hat{I}_e \oplus \hat{J}_e$, this shows that $S_A(b)S_A(a) \in S_A(I_e)$ for all $a \in A$, which establishes the first assertion because the antipode S_A is bijective, as we mentioned in Paragraph 1.3.

(2) Now suppose that $I \subset A$ is an ideal containing e with the property that $S_A(I)$ is an ideal. The very last formula yields in the case $b = e$ that

$$S_A(e)S_A(a) = \frac{1}{|Q_e^\perp||Q_e \cap T_e^\perp|} \sum_{\gamma \in T_e^\perp} \sum_{g \in Q_e^\perp} \gamma(g)S_A(\psi_\gamma(a)\phi_g(e))$$

for all $a \in \hat{I}_e$. But if $a \in \hat{J}_e$, we saw slightly before that $S_A(e)S_A(a) = 0$. As the right-hand side of the last formula also vanishes in this case, this formula also holds if $a \in \hat{J}_e$, and therefore for all $a \in A = \hat{I}_e \oplus \hat{J}_e$. Since $S_A(e)S_A(a) \in S_A(I)$, this implies that

$$\sum_{\gamma \in T_e^\perp} \sum_{g \in Q_e^\perp} \gamma(g)\psi_\gamma(a)\phi_g(e) \in I$$

for all $a \in A$. Because $\psi_\gamma(a)\phi_g(e) = \phi_g(\phi_{g^{-1}}(\psi_\gamma(a))e) = \eta_e(\phi_{g^{-1}}(\psi_\gamma(a)))\phi_g(e)$, this can be written in the form

$$\sum_{g \in Q_e^\perp} \sum_{\gamma \in T_e^\perp} \gamma(g)\eta_e(\phi_{g^{-1}}(\psi_\gamma(a)))\phi_g(e) \in I$$

(3) The elements u_h introduced in Definition 3.2 are in particular defined when $e = e'$ in the terminology used there, and this is the case which we consider here. For $h \in Q_e^\perp$, we insert $a = \phi_{h^{-1}}(u_h)$ into the condition obtained in the previous step. With the help of Corollary 3.2, we then find that the element

$$\begin{aligned} & \sum_{g \in Q_e^\perp} \sum_{\gamma \in T_e^\perp} \gamma(g)\eta_e(\phi_{g^{-1}}(\psi_\gamma(\phi_{h^{-1}}(u_h))))\phi_g(e) \\ &= \sum_{g \in Q_e^\perp} \sum_{\gamma \in T_e^\perp} \gamma(g)\gamma(h)\eta_e(\phi_{g^{-1}}(\phi_{h^{-1}}(u_h)))\phi_g(e) \\ &= |T_e^\perp| \sum_{g \in Q_e^\perp \cap h^{-1}T_e} \eta_e(\phi_{g^{-1}h^{-1}}(u_h))\phi_g(e) \\ &= |T_e^\perp| \sum_{g \in h^{-1}Q_e^\perp \cap h^{-1}T_e} \eta_e(u_h)\phi_g(e) = |T_e^\perp||Q_e^\perp \cap T_e|\phi_{h^{-1}}(e) \end{aligned}$$

is contained in I , and therefore we get that $\phi_{h^{-1}}(e) \in I$ for all $h \in Q_e^\perp$, which shows that $I_e \subset I$, as asserted. \square

This theorem, which should be compared with [30], Lem. 6.3, p. 92, enables us to determine precisely when the image of an ideal under the antipode is again an ideal:

Corollary For an ideal $I \subset A$, the following conditions are equivalent:

1. For all primitive idempotents $e \in I$ and all $g \in Q_e^\perp$, we have $\phi_g(e) \in I$.
2. $S_A(I)$ is an ideal.

Proof. The first condition implies that $I_e \subset I$ for all primitive idempotents $e \in I$, so that

$$I = \sum_{e \in I \cap E} I_e$$

We then have that

$$S_A(I) = \sum_{e \in I \cap E} S_A(I_e)$$

is a sum of ideals by the preceding theorem, and therefore itself an ideal.

Conversely, if $S_A(I)$ is an ideal, we have also by the preceding theorem that $I_e \subset I$ for every primitive idempotent $e \in I$, which is equivalent to the first condition. \square

The decisive property of the ideal I_e is shared by its complement J_e :

Lemma For a primitive idempotent $e \in E$, we have that $S_A(J_e)$ is an ideal.

Proof. We use again the full orbit \hat{O}_e , the associated ideal \hat{I}_e , and its complement \hat{J}_e from Definition 3.1. Since \hat{J}_e is stable under G , the preceding corollary implies that $S_A(\hat{J}_e)$ is an ideal. Now we decompose \hat{O}_e further as a disjoint union of the form

$$\hat{O}_e = \tilde{O}_1 \cup \cdots \cup \tilde{O}_r$$

where $\tilde{O}_1, \dots, \tilde{O}_r$ are the orbits of Q_e^\perp and $\tilde{O}_1 = O_e$ is the orbit of e . By construction, all elements of \hat{O}_e have the same isotropy group as e . If we choose a representative $e_i \in \tilde{O}_i$ for all $i = 1, \dots, r$, where we can choose $e_1 = e$, we therefore have $Q_e^\perp = Q_{e_i}^\perp$, $\tilde{O}_i = O_{e_i}$, and

$$\hat{I}_e = I_{e_1} \oplus \cdots \oplus I_{e_r}$$

Moreover, $S_A(I_{e_i})$ is an ideal by the preceding theorem. Since we have

$$J_e = \hat{J}_e \oplus I_{e_2} \oplus \cdots \oplus I_{e_r}$$

we see that $S_A(J_e) = S_A(\hat{J}_e) \oplus S_A(I_{e_2}) \oplus \cdots \oplus S_A(I_{e_r})$ is again an ideal. \square

3.5 Our considerations so far have not been as symmetric in ϕ_g and ψ_γ as they could have been, as we have used the group Q_e , and not the group T_e , for the definition of the ideal I_e . However, as we pointed out at the end of Paragraph 2.1, the situation is indeed entirely symmetric in this regard, which in view of Theorem 3.4 has the following consequence:

Proposition For a primitive idempotent $e \in E$, we have

$$\{\phi_g(e) \mid g \in Q_e^\perp\} = \{\psi_\gamma(e) \mid \gamma \in T_e^\perp\}$$

Proof. In the same way as in our treatment of Corollary 3.2, we can consider $A^{\text{op cop}} = A^{\text{cop}}$ as a left Yetter-Drinfel'd Hopf algebra over $H^* \cong K[\hat{G}]$. This operation does not change the antipode S_A , so that I_e is still the minimal ideal I containing e with the property that $S_A(I)$ is an ideal. However, this operation exchanges ϕ_g and ψ_γ and consequently T_e and Q_e , and therefore over H^* the definition of I_e would be $I_e := \text{Span}(\{\psi_\gamma(e) \mid \gamma \in T_e^\perp\})$. Since the set of primitive idempotents spanning an ideal is unique, this implies the assertion. \square

It is of course possible to give an alternative proof of this proposition by adapting the proof of Theorem 3.4 to show that the ideal $\text{Span}(\{\psi_\gamma(e) \mid \gamma \in T_e^\perp\})$ is also the minimal ideal I containing e with the property that $S_A(I)$ is an ideal. We note that this proposition generalizes [30], Prop. 6.4, p. 93, where the argument was based on Clifford theory applied to the Radford biproduct. While it is possible to generalize the proof given there to the current situation, the proof that we have given here is considerably simpler.

Obviously, the ideals I_e and $S_A(I_e)$ are in general not equal, as these two sets are already usually distinct in the case of ordinary Hopf algebras, i.e., trivial Yetter-Drinfel'd Hopf algebras. However, we can say the following:

Corollary $S_A^2(I_e) = I_e$

Proof. In the last step of the proof of Proposition 1.5, we have already observed that $S_A^2 = \theta_A^{-1}$, the inverse ribbon transformation defined in [28], Par. 3.5, p. 441. In our situation, the formula given there yields

$$\theta_A^{-1}(a) = a^{(1)} \cdot a^{(2)}$$

which in view of Corollary 2.1 means for $a \in I_e$ that

$$\theta_A^{-1}(a) = \frac{1}{|G|} \sum_{\gamma \in \hat{G}} \sum_{g \in Q_e^\perp} \gamma(g^{-1}) \phi_g(\psi_\gamma(a))$$

In the case where $\gamma \notin Q_e T_e^\perp$, we can argue as in the proof of Lemma 2.1 to see that $\sum_{g \in Q_e^\perp} \gamma(g^{-1}) \phi_g(\psi_\gamma(a)) = 0$. The formula above therefore reduces to

$$\theta_A^{-1}(a) = \frac{1}{|G|} \sum_{\gamma \in Q_e T_e^\perp} \sum_{g \in Q_e^\perp} \gamma(g^{-1}) \phi_g(\psi_\gamma(a))$$

Now I_e is stable under Q_e^\perp by definition and under $Q_e T_e^\perp$ by the preceding proposition. Therefore, the last equation shows that $S_A^2(a) = \theta_A^{-1}(a) \in I_e$. \square

The last displayed formula in the preceding proof is not entirely symmetric in g and γ . However, it would be possible to bring this formula into a symmetric form by using, as in the proof of Lemma 2.1, the group homomorphism $T_e^\perp \times Q_e \rightarrow Q_e T_e^\perp$, $(\gamma, \gamma') \mapsto \gamma\gamma'$. We have not presented this step because it is logically not necessary to prove the preceding corollary.

As the image of an ideal under the antipode is in general not an ideal, we cannot expect that the image of a primitive idempotent under the antipode is again a primitive idempotent. The following lemma describes exactly when this happens:

Lemma Suppose that $e \in E$ is a primitive idempotent. Then $S_A(e)$ is a primitive idempotent if and only if the index of e is 1.

Proof. If $S_A(e)$ is a primitive idempotent, then $I := Ke$ is an ideal containing e with the property that $S_A(I)$ is an ideal. Theorem 3.4 therefore implies that $I_e \subset I$, so that $|G_e| = \dim(I_e) = 1$. Conversely, $|G_e| = 1$ implies $Q_e^\perp = T_e \cap Q_e^\perp$ and therefore $Q_e^\perp \subset T_e$, so that $T_e^\perp \subset Q_e$. Now we saw in the second step of the proof of Theorem 3.4 that

$$S_A(e)S_A(a) = \frac{1}{|Q_e^\perp||Q_e \cap T_e^\perp|} \sum_{\gamma \in T_e^\perp} \sum_{g \in Q_e^\perp} \gamma(g) S_A(\psi_\gamma(a)\phi_g(e))$$

for all $a \in A$, which then reduces to

$$\begin{aligned} S_A(e)S_A(a) &= \frac{1}{|T_e^\perp|} \sum_{\gamma \in T_e^\perp} S_A(\psi_\gamma(a)e) \\ &= \frac{1}{|T_e^\perp|} \sum_{\gamma \in T_e^\perp} \eta_e(\psi_\gamma(a)) S_A(e) = \eta_e(a) S_A(e) \end{aligned}$$

Because the antipode S_A is bijective, as we noted in Paragraph 1.3, this shows on the one hand that $KS_A(e)$ is a one-dimensional ideal, but on the other hand it also shows for $a = e$ that $S_A(e)^2 = S_A(e)$, so that $S_A(e)$ is an idempotent. Since the ideal that it generates is one-dimensional, $S_A(e)$ is primitive (cf. [13], Prop. (21.8), p. 320). \square

Our situation has an interesting feature: For the elements $g \in Q_e^\perp$, the mappings ϕ_g preserve both I_e and $S_A(I_e)$ (as do the mappings ψ_γ for $\gamma \in T_e^\perp$). Inside these ideals, they permute the primitive idempotents, so that we have two permutation representations of Q_e^\perp . Since $S_A \circ \phi_g = \phi_g \circ S_A$ by the H -linearity of the antipode, these two representations are isomorphic as linear representations. However, we have seen above that the antipode usually does not map primitive

idempotents to primitive idempotents, and is therefore not an isomorphism of permutation representations.

In general, two permutation representations that are isomorphic as linear representations need not be isomorphic as permutation representations. In [9], Kap. V, Bsp. 20.10, p. 606, B. Huppert gives two examples of this phenomenon. In one of these examples, the group is abelian, whereas in the other example, which he attributes to H. Wielandt, the two permutation representations are transitive, but the group is not abelian. However, in our situation, this phenomenon cannot occur, because two permutation representations of an abelian group that are isomorphic as linear representations are isomorphic as permutation representations if one of them is transitive. This is not very hard to see: If a group element acts as the identity in one representation, then also in the other, because the linear representations are isomorphic. Moreover, this group element has in both permutation representations the same number of fixed points, because this number is just its trace in the corresponding linear representation. But in the transitive permutation representation, a group element that has one fixed point already acts as the identity, because all stabilizers are then conjugate and, as the group is abelian, even equal. We therefore see that this property also holds for the other permutation representation that was not assumed to be transitive, although this one now also turns out to be transitive for cardinality reasons. This shows that both permutation representations are regular in the sense of [9], Kap. I, Def. 5.12, p. 27, i.e., isomorphic to the permutation representation on the cosets of their common kernel, and in particular isomorphic to each other (cf. [9], Kap. I, Satz 5.13, p. 27; [12], Par. 4.1.3, p. 78).

3.6 As we have already mentioned in Paragraph 3.1, we have $\check{J}_e^\perp = \text{Span}(\check{U}_e)$. The decisive property of this space is the following:

Theorem $\text{Span}(\check{U}_e)$ is a Yetter-Drinfel'd Hopf subalgebra of A^* .

Proof. We have also pointed out in Paragraph 3.1 that \check{U}_e is stable under both G and \check{G} , so that \check{J}_e^\perp is a submodule and a subcomodule. As it is spanned by group-like elements, \check{J}_e^\perp is in addition a subcoalgebra. It follows from Corollary 3.4 that $S_A(\check{I}_e)$ and $S_A(\check{J}_e)$ are ideals. Since the primitive idempotents that span $S_A(\check{I}_e)$ are clearly stabilized by T_e and Q_e , we have $S_A(\check{I}_e) \subset \check{I}_e$ and therefore $S_A(\check{I}_e) = \check{I}_e$ by dimension considerations. Because

$$A = S_A(\check{I}_e) \oplus S_A(\check{J}_e) = \check{I}_e \oplus S_A(\check{J}_e)$$

this implies that $S_A(\check{J}_e) = \check{J}_e$, which in turn implies that $S_A^*(\check{J}_e^\perp) = \check{J}_e^\perp$.

Since \check{U}_e evidently contains the counit ε_A , it remains to be shown that $\text{Span}(\check{U}_e)$ is multiplicatively closed. To see this, we consider two primitive idempotents e' and e'' in \check{O}_e and define, as in Paragraph 3.2, the sets

$$O' := \{\phi_g(e') \mid g \in Q_{e''}^\perp\} \quad O'' := \{\psi_\gamma(e'') \mid \gamma \in T_{e'}^\perp\}$$

Then we know from Lemma 3.2 that $m := |O'| = |O''|$ and from Theorem 3.3 that there are distinct characters $\omega_1, \dots, \omega_m$ such that

$$\text{Span}(\{\eta_{\tilde{e}'}\eta_{\tilde{e}''} \mid \tilde{e}' \in O', \tilde{e}'' \in O''\}) = \text{Span}(\omega_1, \dots, \omega_m)$$

For $g \in T_e$ and $\tilde{e}' \in O'$, we have $\phi_g(\tilde{e}') = \tilde{e}'$ and therefore $\phi_g^*(\eta_{\tilde{e}'}) = \eta_{\tilde{e}'}$. For exactly the same reason, we have $\phi_g^*(\eta_{\tilde{e}''}) = \eta_{\tilde{e}''}$ for $\tilde{e}'' \in O''$. These two statements together show that $\phi_g^*(\omega_k) = \omega_k$ for all $k = 1, \dots, m$. A very similar argument shows that $\psi_\gamma^*(\omega_k) = \omega_k$ for all $k = 1, \dots, m$ and all $\gamma \in Q_e$, so that $\omega_k \in \check{U}_e$. Since in particular

$$\eta_{\tilde{e}'}\eta_{\tilde{e}''} \in \text{Span}(\omega_1, \dots, \omega_m) \subset \text{Span}(\check{U}_e)$$

this implies the assertion. \square

By construction, T_e and Q_e act trivially on \check{U}_e . Therefore, Proposition 2.2 implies the following:

Corollary $\text{Span}(\check{U}_e)$ is a Yetter-Drinfel'd Hopf algebra over $K[G_e]$.

Proof. This follows directly from Proposition 2.2, although this proposition was stated for left Yetter-Drinfel'd Hopf algebras, whereas here we have right Yetter-Drinfel'd Hopf algebras. However, we can pass from one to the other with the help of Lemma 1.3. \square

Consequently, primitive idempotents of index 1 give rise to trivial Yetter-Drinfel'd Hopf subalgebras:

Proposition For a primitive idempotent $e \in E$ of index 1, \check{U}_e is a subgroup of the group of units of A^* . Its group ring $K[\check{U}_e] = \text{Span}(\check{U}_e) \subset A^*$ is therefore a trivial right Yetter-Drinfel'd Hopf subalgebra of A^* .

Proof. If $|G_e| = 1$, then the preceding corollary yields that $\text{Span}(\check{U}_e)$ is a Yetter-Drinfel'd Hopf subalgebra over $K[G_e] \cong K$. The corresponding quasisymmetry is clearly the ordinary flip of tensor factors, so that $\text{Span}(\check{U}_e)$ is trivial, i.e., an ordinary Hopf algebra. It is obviously spanned by the set \check{U}_e of group-like elements, which therefore form a group. \square

Although the preceding argument is complete, it is possible to give a slightly more explicit proof that \check{U}_e is a group. As we pointed out in the proof of the preceding theorem, \check{U}_e contains the counit ε_A . From the proof of Lemma 3.5, we know that $|G_e| = 1$ implies $Q_e^\perp \subset T_e$. If $e' \in \check{O}_e$, so that $T_e \subset T_{e'}$ and $Q_e \subset Q_{e'}$, we therefore have

$$Q_{e'}^\perp \subset Q_e^\perp \subset T_e \subset T_{e'}$$

so that e' has also index 1. Now Lemma 3.5 yields that $S_A(e')$ is again a primitive idempotent, which is clearly contained in \check{O}_e . This shows that $S_A(\check{O}_e) = \check{O}_e$,

and dually we have $S_A^*(\check{U}_e) = \check{U}_e$. Since $\eta_{e'}^{-1} = S_A^*(\eta_{e'})$ for $e' \in \check{O}_e$, we see that \check{U}_e contains the inverses of all its elements.

To show that \check{U}_e is multiplicatively closed, we suppose that e' and e'' are two primitive idempotents in \check{O}_e . We then have

$$Q_{e''}^\perp \subset Q_e^\perp \subset T_e \subset T_{e'}$$

and therefore Corollary 3.3 implies that $\eta_{e'}\eta_{e''}$ is again a character. Since this character is clearly preserved by T_e and Q_e , we have $\eta_{e'}\eta_{e''} \in \check{U}_e$. From Corollary 3.3, we also get that $\sigma_{A^*, A^*}(\eta_{e'} \otimes \eta_{e''}) = \eta_{e''} \otimes \eta_{e'}$, which means that $\text{Span}(\check{U}_e)$ is trivial.

3.7 In Paragraph 3.3, we have investigated the product of two characters belonging to arbitrary primitive idempotents e and e' . The next step is, exactly as in Paragraph 6.7 of [30], to analyze the special case that $e' \in S_A(I_e)$. As we have discussed at the end of Paragraph 3.5, we then have $T_e = T_{e'}$, $Q_e = Q_{e'}$, and $I_{e'} = S_A(I_e)$. By Proposition 3.5, the orbits O and O' introduced at the beginning of Paragraph 3.2 are therefore equal to O_e and $O_{e'}$, respectively, and the ideals I and I' also introduced there are consequently equal to I_e and $I_{e'}$. Proposition 3.5 also shows that both I_e and $I_{e'}$ are invariant under T_e^\perp and Q_e^\perp .

If $m = |G_e| = |G_{e'}|$ is the index of e and e' , we have already seen in Theorem 3.3 and the discussion afterwards that there are unique distinct characters $\omega_1, \dots, \omega_m \in A^*$ with the property that $\eta_e\eta_{e'} \in \text{Span}(\omega_1, \dots, \omega_m)$. By definition, there are corresponding idempotents $e''_1, \dots, e''_m \in E$ so that $\omega_k = \eta_{e''_k}$. In our case, when $e' \in S_A(I_e)$, these characters have additional properties, besides those already listed in Theorem 3.3:

Proposition

1. $\{\omega_1, \dots, \omega_m\} \subset \check{U}_e$
2. For $\gamma \in T_e^\perp$, $\{\omega_1, \dots, \omega_m\}$ is stable under ψ_γ^* .
3. For $g \in Q_e^\perp$, $\{\omega_1, \dots, \omega_m\}$ is stable under ϕ_g^* .
4. For some $i \leq m$, we have $\omega_i = \varepsilon_A$.
5. Unless $m = 1$, the index of ω_j is strictly less than m for all $j \leq m$.

Proof. (1) The second and the third assertion follow directly from Theorem 3.3. This theorem also implies that

$$\text{Span}(U_e U_{e'}) = \text{Span}(\omega_1, \dots, \omega_m)$$

Since $U_e \subset \check{U}_e$ and $U_{e'} \subset \check{U}_e$ by construction, Theorem 3.6 implies that

$$\text{Span}(\omega_1, \dots, \omega_m) \subset \text{Span}(\check{U}_e)$$

Because distinct group-like elements are linearly independent, as we have already mentioned in the proof of Theorem 3.3, this yields the first assertion.

(2) In order to prove the fourth assertion, we recall from Proposition 3.1 that $S_A^{-1}(e') = \Lambda_{A(1)}\eta_{e'}(\Lambda_{A(2)})$, which is contained in I_e by construction. For the restriction of the module structure on I_e described in Proposition 3.2 to A along Δ_A , we therefore have

$$\begin{aligned} a.S_A^{-1}(e') &= \Delta_A(a).S_A^{-1}(e') = a_{(1)}(a_{(2)}^{(1)}.S_A^{-1}(e'))\eta_{e'}(a_{(2)}^{(2)}) \\ &= a_{(1)}(a_{(2)}^{(1)}.\Lambda_{A(1)})\eta_{e'}(\Lambda_{A(2)})\eta_{e'}(a_{(2)}^{(2)}) \\ &= a_{(1)}(a_{(2)}^{(1)}.\Lambda_{A(1)})\eta_{e'}(a_{(2)}^{(2)}\Lambda_{A(2)}) \\ &= (a\Lambda_A)_{(1)}\eta_{e'}((a\Lambda_A)_{(2)}) = \varepsilon_A(a)\Lambda_{A(1)}\eta_{e'}(\Lambda_{A(2)}) = \varepsilon_A(a)S_A^{-1}(e') \end{aligned}$$

From the proof of Theorem 3.3, we know that the characters $\omega_1, \dots, \omega_m$ arise from the decomposition of this A -module structure on I_e into one-dimensional submodules. The preceding computation shows that one of these submodules is $KS_A^{-1}(e')$ and that the corresponding character is ε_A . Therefore, we must have $\omega_i = \varepsilon_A$ for some $i \leq m$, so that $e''_i = \Lambda_A$.

(3) To prove the fifth assertion, we get from the first assertion that $e''_j \in \check{O}_e$ and hence $T_e \subset T_{e''_j}$ and $Q_e \subset Q_{e''_j}$, which in turn implies that $T_{e''_j}^\perp \subset T_e^\perp$ and $Q_{e''_j}^\perp \subset Q_e^\perp$. From the third assertion, we know that $\{e''_1, \dots, e''_m\}$ is stable under Q_e^\perp , and therefore under $Q_{e''_j}^\perp$. So the orbit $O_{e''_j}$ of e''_j under the action of $Q_{e''_j}^\perp$ is contained in $\{e''_1, \dots, e''_m\}$, which shows that the index $|O_{e''_j}|$ of e''_j is less than or equal to m . To show that it is strictly less than m , we distinguish two cases: If $j = i$, we have $e''_i = \Lambda_A$, which has index 1, and 1 is less than m by assumption. If $j \neq i$, then $e''_i \notin O_{e''_j}$, so $|O_{e''_j}| < m$, as asserted. \square

This proposition shows that after renumbering the characters, we can, and will, assume that $\omega_1 = \varepsilon_A$, so that $e''_1 = \Lambda_A$. Its proof shows that for the corresponding eigenvector v_1 introduced in Paragraph 3.3, we can choose $v_1 = S_A^{-1}(e')$.

As pointed out at the beginning of this paragraph, we have $S_A(I_e) = I_{e'}$. The statement $S_A^2(I_e) = I_e$ in Corollary 3.5 therefore means that $S_A(I_{e'}) = I_e$. In addition, we get from $A = I_e \oplus J_e$ that

$$A = S_A(I_e) \oplus S_A(J_e) = I_{e'} \oplus S_A(J_e)$$

Since $S_A(J_e)$ is an ideal by Lemma 3.4, it must be the unique ideal that complements $I_{e'}$; in other words, we have $S_A(J_e) = J_{e'}$. A similar argument shows that $S_A(J_{e'}) = J_e$. These observations are used in the proof of the following lemma:

Lemma $\text{Span}(\omega_1, \dots, \omega_m)$ is stable under the antipode S_A^* .

Proof. We have already noted in Paragraph 3.1 that

$$J_e^\perp = \text{Span}(U_e) \quad J_{e'}^\perp = \text{Span}(U_{e'})$$

and the discussion above implies that $S_A^*(J_{e'}^\perp) = J_e^\perp$ and $S_A^*(J_e^\perp) = J_{e'}^\perp$. Moreover, we know from the proof of the preceding proposition that

$$\text{Span}(U_e U_{e'}) = \text{Span}(\omega_1, \dots, \omega_m)$$

Let us now suppose that $\tilde{e} \in O_e$ and $\tilde{e}' \in O_{e'}$. By Proposition 1.3, A^* is a right Yetter-Drinfel'd Hopf algebra over H with antipode S_A^* , and from the relation between antipode and multiplication also stated in Paragraph 1.3 together with the formulas for the quasisymmetry given after Lemma 2.1 we get

$$S_A^*(\eta_{\tilde{e}} \eta_{\tilde{e}'}) = \frac{1}{|Q_e^\perp| |Q_e \cap T_{e'}^\perp|} \sum_{\gamma \in T_{e'}^\perp} \sum_{g \in Q_e^\perp} \gamma(g^{-1}) S_A^*(\psi_\gamma^*(\eta_{\tilde{e}'})) S_A^*(\phi_g^*(\eta_{\tilde{e}}))$$

For $\gamma \in T_{e'}^\perp$ and $g \in Q_e^\perp$, we have $\psi_\gamma^*(\eta_{\tilde{e}'}) \in J_{e'}^\perp$ and $\phi_g^*(\eta_{\tilde{e}}) \in J_e^\perp$, because J_e and $J_{e'}$ are stable under $Q_e^\perp = Q_{e'}^\perp$ by construction and under $T_{e'}^\perp = T_{e'}^\perp$ by Proposition 3.5. Therefore, the above formula shows that $S_A^*(\eta_{\tilde{e}} \eta_{\tilde{e}'})$ is contained in the span of $J_e^\perp J_{e'}^\perp$, which is $\text{Span}(\omega_1, \dots, \omega_m)$, as asserted. \square

We note that, since $S_A^*(\omega_k) = \omega_k^{-1}$, this lemma can also be stated in the form

$$\text{Span}(\omega_1^{-1}, \dots, \omega_m^{-1}) = \text{Span}(\omega_1, \dots, \omega_m)$$

The spaces J_e^\perp and $J_{e'}^\perp$ just considered are preserved under left and right multiplication by ω_k :

Theorem For all $k = 1, \dots, m$, we have

$$\omega_k J_e^\perp = J_e^\perp \omega_k = J_e^\perp \quad \omega_k J_{e'}^\perp = J_{e'}^\perp \omega_k = J_{e'}^\perp$$

Moreover, we have $\text{Span}(U_{e'} U_e) = \text{Span}(\omega_1, \dots, \omega_m)$.

Proof. (1) For $\tilde{e} \in O_e$, we have that $\eta_{\tilde{e}}^{-1} = S_A^*(\eta_{\tilde{e}}) \in S_A^*(J_e^\perp) = J_{e'}^\perp$ and therefore

$$J_e^\perp \eta_{\tilde{e}}^{-1} \subset J_e^\perp J_{e'}^\perp \subset \text{Span}(\omega_1, \dots, \omega_m)$$

Since the spaces on the left and on the right have the same dimension, we get $J_e^\perp \eta_{\tilde{e}}^{-1} = \text{Span}(\omega_1, \dots, \omega_m)$ and consequently $J_e^\perp = \text{Span}(\omega_1 \eta_{\tilde{e}}, \dots, \omega_m \eta_{\tilde{e}})$. This shows that $\omega_k \eta_{\tilde{e}} \in J_e^\perp$, which yields $\omega_k J_e^\perp = J_e^\perp$.

(2) Similarly, we have for $\tilde{e}' \in O_{e'}$ that $\eta_{\tilde{e}'}^{-1} = S_A^*(\eta_{\tilde{e}'}) \in S_A^*(J_{e'}^\perp) = J_e^\perp$ and therefore

$$\eta_{\tilde{e}'}^{-1} J_{e'}^\perp \subset J_e^\perp J_{e'}^\perp \subset \text{Span}(\omega_1, \dots, \omega_m)$$

Again by comparing dimensions, we get $\eta_{\tilde{e}'}^{-1} J_{e'}^\perp = \text{Span}(\omega_1, \dots, \omega_m)$ and consequently $J_{e'}^\perp = \text{Span}(\eta_{\tilde{e}'} \omega_1, \dots, \eta_{\tilde{e}'} \omega_m)$. This shows that $\eta_{\tilde{e}'} \omega_k \in J_{e'}^\perp$, which yields $J_{e'}^\perp \omega_k = J_{e'}^\perp$.

(3) By applying Theorem 3.3 in the case where the idempotents are equal, we see that $\text{Span}(U_e U_e)$ is an m -dimensional space. Hence we have

$$J_e^\perp \eta_e = \text{Span}(U_e \eta_e) = \text{Span}(\eta_e U_e) = \eta_e J_e^\perp$$

Since we saw in the first step that $\text{Span}(\omega_1 \eta_e, \dots, \omega_m \eta_e) = J_e^\perp$, it follows that $\text{Span}(\eta_e \omega_1 \eta_e, \dots, \eta_e \omega_m \eta_e) = \eta_e J_e^\perp = J_e^\perp \eta_e$.

(4) As we saw above, we have not only $I_{e'} = S_A(I_e)$, but also $I_e = S_A(I_{e'})$. We can therefore interchange the roles of e and e' and find characters $\omega'_1, \dots, \omega'_m$ with the property that

$$\text{Span}(U_{e'} U_e) = \text{Span}(\omega'_1, \dots, \omega'_m)$$

which by the first two steps satisfy $\omega'_k J_{e'}^\perp = J_{e'}^\perp$ and $J_{e'}^\perp \omega'_k = J_{e'}^\perp$, and by the second step also $\text{Span}(\eta_e \omega'_1, \dots, \eta_e \omega'_m) = J_e^\perp$. This implies

$$\text{Span}(\eta_e \omega'_1 \eta_e, \dots, \eta_e \omega'_m \eta_e) = J_e^\perp \eta_e$$

(5) Comparing the last two steps, we get

$$\text{Span}(\eta_e \omega_1 \eta_e, \dots, \eta_e \omega_m \eta_e) = \text{Span}(\eta_e \omega'_1 \eta_e, \dots, \eta_e \omega'_m \eta_e)$$

which in turn clearly implies $\text{Span}(\omega_1, \dots, \omega_m) = \text{Span}(\omega'_1, \dots, \omega'_m)$ by multiplying with η_e^{-1} on the left and on the right. As we have already recalled in the proof of the proposition above, distinct group-like elements are linearly independent, and hence we must have $\{\omega_1, \dots, \omega_m\} = \{\omega'_1, \dots, \omega'_m\}$. For a given $k = 1, \dots, m$, we can therefore find $l = 1, \dots, m$ so that $\omega_k = \omega'_l$, and then have $\omega_k J_{e'}^\perp = \omega'_l J_{e'}^\perp = J_{e'}^\perp$ and $J_{e'}^\perp \omega_k = J_{e'}^\perp \omega'_l = J_{e'}^\perp$, as asserted. \square

This theorem obviously implies that multiplication by the inverse of ω_k also preserves these spaces; i.e., we have

$$\omega_k^{-1} J_e^\perp = J_e^\perp \omega_k^{-1} = J_e^\perp \quad \omega_k^{-1} J_{e'}^\perp = J_{e'}^\perp \omega_k^{-1} = J_{e'}^\perp$$

3.8 In the last paragraph, we have considered two primitive idempotents e and e' that satisfy the restriction $e' \in S_A(I_e)$, and we have obtained distinct characters $\omega_1, \dots, \omega_m$ with the property that

$$\text{Span}(U_e U_{e'}) = \text{Span}(U_{e'} U_e) = \text{Span}(\omega_1, \dots, \omega_m)$$

where $m = |G_e| = |G_{e'}|$. For a given primitive idempotent $e \in E$, this space does not depend on the choice of the primitive idempotent $e' \in S_A(I_e)$, because two different choices of such idempotents nonetheless generate the same orbit $O_{e'}$. Therefore, the following definition is meaningful:

Definition For a primitive idempotent $e \in E$, the space $\text{Span}(U_e U_{e'})$, where e' is some primitive idempotent in $S_A(I_e)$, is called the core of e , or alternatively the core of η_e .

As recalled in the preceding paragraph, the dual space A^* is a right Yetter-Drinfel'd Hopf algebra over H . As we will see in a moment that the core $\text{Span}(\omega_1, \dots, \omega_m)$ is multiplicatively closed, it seems reasonable to conjecture that the core is a Yetter-Drinfel'd Hopf subalgebra of A^* . This, however, cannot be the case, as it is not invariant under the entire group G , but only, as we have seen in Proposition 3.7, under the subgroup Q_e^\perp . Nevertheless, it is a Yetter-Drinfel'd Hopf subalgebra over a different group:

Theorem The core $\text{Span}(\omega_1, \dots, \omega_m)$ is a Yetter-Drinfel'd Hopf subalgebra of the right $K[G_e]$ -Yetter-Drinfel'd Hopf algebra $\text{Span}(\check{U}_e)$.

Proof. (1) First, we have to verify that the core is multiplicatively closed. But this follows from Theorem 3.7, as we have

$$\begin{aligned} (U_e U_{e'}) (U_e U_{e'}) &\subset U_e \text{Span}(\omega_1, \dots, \omega_m) U_{e'} \\ &\subset J_e^\perp \text{Span}(\omega_1, \dots, \omega_m) J_{e'}^\perp \subset J_e^\perp J_{e'}^\perp \subset \text{Span}(\omega_1, \dots, \omega_m) \end{aligned}$$

(2) From the first assertion in Proposition 3.7, we know that the core is contained in $\text{Span}(\check{U}_e)$, and from its fourth assertion we know that the core contains the counit ε_A and is therefore a unital subalgebra of $\text{Span}(\check{U}_e)$. Because $\omega_1, \dots, \omega_m$ are group-like elements of the dual, the core is also a subcoalgebra. Again by Proposition 3.7, our space is stable under the maps ϕ_g^* and ψ_γ^* for $g \in Q_e^\perp$ and $\gamma \in T_e^\perp$. The action of Q_e^\perp clearly factors over $G_e = Q_e^\perp / (T_e \cap Q_e^\perp)$, which means that the core is a right $K[G_e]$ -submodule of $\text{Span}(\check{U}_e)$. Similarly, the action of T_e^\perp factors over $T_e^\perp / (Q_e \cap T_e^\perp)$, and we saw in Lemma 2.2 that this group is isomorphic to the character group \hat{G}_e of G_e . From the way how the coaction was constructed in Paragraph 2.2, we see that the fact that the core is a $K[T_e^\perp / (Q_e \cap T_e^\perp)]$ -submodule means that it is also a $K[G_e]$ -subcomodule. Finally, Lemma 3.7 implies that $\text{Span}(\omega_1, \dots, \omega_m)$ is stable under the antipode and hence a Yetter-Drinfel'd Hopf subalgebra of $\text{Span}(\check{U}_e)$. \square

As we have pointed out above, the core is not a Yetter-Drinfel'd Hopf subalgebra of A^* . However, M. Takeuchi has introduced a version of the notion of a braided Hopf algebra which does not use the quasisymmetry of some outside category, but rather lists this map as part of the data of the braided Hopf algebra (cf. [33], Def. 5.1, p. 310). Since they are both Yetter-Drinfel'd Hopf algebras, although over different Hopf algebras, both the core and A^* are Hopf algebras in Takeuchi's sense (cf. [33], Thm. 5.7, p. 314). Furthermore, the proof of Proposition 2.2 shows that the core is a Yang-Baxter subspace in Takeuchi's terminology (cf. [33], Eq. (6.3), p. 314). However, in this terminology, it is not a categorical Yang-Baxter subspace (cf. [33], Eq. (6.4), p. 315).

As Takeuchi explains, Scharfschwerdt's version of the Nichols-Zoeller theorem cited in Paragraph 1.5 can be used to establish freeness for categorical braided Hopf subalgebras in the sense just discussed (cf. [33], Thm. 7.3, p. 316). As the

core is not categorical, this result does not apply directly to the core viewed as a subalgebra of A^* . Nonetheless, there are two ways to arrive at the same conclusion:

Corollary A^* is free as a left and right module over $\text{Span}(\omega_1, \dots, \omega_m)$. In particular, the index m of e divides $\dim(A)$.

Proof. We have already seen in the proof of the preceding theorem that the core is a unital subalgebra, and also a subcoalgebra, of A^* . Although the module and the comodule structure of both the core and A^* are on the right, Lemma 1.3 implies that Theorem 1.5 also holds for right Yetter-Drinfel'd Hopf algebras, and so this theorem immediately yields the assertion. \square

However, there is a second proof of this corollary that does not rely on the refined version of the Nichols-Zoeller theorem given in Theorem 1.5, but only requires the version of this theorem for Yetter-Drinfel'd Hopf algebras by B. Scharfschwerdt mentioned above and cited in Paragraph 1.5: By Theorem 3.6, $\text{Span}(\check{U}_e)$ is a Yetter-Drinfel'd Hopf subalgebra of A^* , both considered as Yetter-Drinfel'd Hopf algebras over $K[G]$. Therefore, A^* is free as a left and right module over $\text{Span}(\check{U}_e)$. But by Corollary 3.6, $\text{Span}(\check{U}_e)$ can also be considered as a Yetter-Drinfel'd Hopf algebra over $K[G_e]$, and by the preceding theorem the core is a Yetter-Drinfel'd Hopf subalgebra of $\text{Span}(\check{U}_e)$, both considered as Yetter-Drinfel'd Hopf algebras over $K[G_e]$. Therefore, $\text{Span}(\check{U}_e)$ is free as a left and right module over $\text{Span}(\omega_1, \dots, \omega_m)$. Since freeness is transitive, this proves the preceding corollary.

3.9 We are now prepared to derive our main results. Before we state them, we first recall that we are considering a commutative semisimple left Yetter-Drinfel'd Hopf algebra over the group ring $K[G]$ of a finite abelian group G . The base field K is assumed to be algebraically closed of characteristic zero. In this situation, we can say the following:

Theorem If $\dim(A)$ and $|G|$ are relatively prime, then A is trivial.

Proof. (1) The index $|G_e|$ of a primitive idempotent e divides $|G|$, and we have shown in Corollary 3.8 that $|G_e|$ divides $\dim(A)$. Hence our assumption implies that every primitive idempotent has index 1. Proposition 3.6 therefore yields that \check{U}_e is a group and that its group ring $K[\check{U}_e] = \text{Span}(\check{U}_e)$ is a trivial Yetter-Drinfel'd Hopf subalgebra of A^* .

(2) We now consider two primitive idempotents e and e' of A that are not necessarily related in any way. It follows from Theorem 3.3 that

$$\text{Span}(\{\phi_g^*(\eta_e)\eta_{e'} \mid g \in Q_{e'}^\perp\}) = \text{Span}(\{\eta_e \psi_\gamma^*(\eta_{e'}) \mid \gamma \in T_e^\perp\})$$

because the spanning sets on both sides of this equation are linearly independent and have by Lemma 3.2 the same number of elements. Multiplying by η_e^{-1} from the left and by $\eta_{e'}^{-1}$ from the right, we get that

$$\text{Span}(\{\eta_e^{-1}\phi_g^*(\eta_e) \mid g \in Q_{e'}^\perp\}) = \text{Span}(\{\psi_\gamma^*(\eta_{e'})\eta_{e'}^{-1} \mid \gamma \in T_e^\perp\})$$

As the left-hand side is a subset of $K[\check{U}_e]$ and the right-hand side is a subset of $K[\check{U}_{e'}]$, the spanning sets on both sides are now group-like elements. Since distinct group-like elements in any coalgebra are linearly independent, as we already mentioned in the proof of Theorem 3.3, we get the stronger statement that

$$\{\eta_e^{-1}\phi_g^*(\eta_e) \mid g \in Q_{e'}^\perp\} = \{\psi_\gamma^*(\eta_{e'})\eta_{e'}^{-1} \mid \gamma \in T_e^\perp\}$$

In particular, for every $g \in Q_{e'}^\perp$ there exists $\gamma \in T_e^\perp$ such that

$$\eta_e^{-1}\phi_g^*(\eta_e) = \psi_\gamma^*(\eta_{e'})\eta_{e'}^{-1}$$

If we introduce the element $\eta' := \psi_\gamma^*(\eta_{e'})\eta_{e'}^{-1} \in \check{U}_{e'}$, which is invariant under $g \in Q_{e'}^\perp \subset T_{e'}$, we can write the last equation in the form $\phi_g^*(\eta_e) = \eta_e\eta'$. More generally, we have for all nonnegative integers $i \in \mathbb{N}_0$ that

$$\phi_{g^i}^*(\eta_e) = \eta_e\eta'^i$$

This is obvious for $i = 0$, holds for $i = 1$ by construction, and then follows inductively, since

$$\phi_{g^{i+1}}^*(\eta_e) = \phi_g^*(\eta_e\eta'^i) = \phi_g^*(\eta_e)\phi_g^*(\eta'^i) = \phi_g^*(\eta_e)\eta'^i = \eta_e\eta'^{i+1}$$

(3) Now let k be the order of $g \in G$, so that $g^k = 1$. Then we have

$$\eta_e = \phi_{g^k}^*(\eta_e) = \eta_e\eta'^k$$

and therefore $\eta'^k = 1$. So the order of η' divides k , which divides the order of G . But the order of η' also divides the order of $\check{U}_{e'}$, which is the dimension of $K[\check{U}_{e'}]$. The dimension of $K[\check{U}_{e'}]$ in turn divides the dimension of A by the Nichols-Zoeller theorem for Yetter-Drinfel'd Hopf algebras cited in Paragraph 1.5 (the refined version given in Theorem 1.5 is not necessary here, although it also yields the result). Because by assumption these numbers are relatively prime, the order of η' must be 1. Therefore we have $\eta' = 1$ and $\phi_g^*(\eta_e) = \eta_e$. This shows that η_e is invariant under $Q_{e'}^\perp$, which means that $Q_{e'}^\perp \subset T_e$. Now Corollary 3.3 implies that

$$\sigma_{A^*, A^*}(\eta_e \otimes \eta_{e'}) = \eta_{e'} \otimes \eta_e$$

Since the characters form a basis of A^* , this shows that A^* is trivial as a right Yetter-Drinfel'd Hopf algebra. But as we know from Paragraph 1.2 that $\sigma_{A, A}$ and σ_{A^*, A^*} are adjoints of each other, this implies that A is trivial, as asserted. \square

As already mentioned in the introduction, this result generalizes [30], Cor. 6.7, p. 100. It may be worth pointing out that the assumption that K is algebraically closed is in fact not necessary: According to Definition 1.3, triviality means that the equation $\sigma_{A,A}(a \otimes a') = a' \otimes a$ holds for all $a, a' \in A$. The validity of this equation does not depend on the base field. We can therefore enlarge the base field to its algebraic closure to decide this question, because our assumptions will still be satisfied over the enlarged base field. This holds in particular for the semisimplicity assumption, as we discussed in Paragraph 1.5.

We now return to the situation where K is an algebraically closed field of characteristic zero, but consider instead a finite-dimensional cocommutative cosemisimple right Yetter-Drinfel'd Hopf algebra A over the group ring $K[G]$ of a finite abelian group G . Although A itself need not be trivial, it contains at least a trivial part:

Proposition If $\dim(A) > 1$, then A contains a trivial Yetter-Drinfel'd Hopf subalgebra B with $\dim(B) > 1$.

Proof. If we can find a primitive idempotent $e \in A^*$ of index 1 that is different from the integral, then Proposition 3.6 yields that $B := K[\check{U}_e] \subset A^{**} \cong A$ is a trivial Yetter-Drinfel'd Hopf subalgebra. As B contains both the counit and η_e , we have $\dim(B) > 1$.

In the case where every primitive idempotent has index 1, we can obviously find such an idempotent. Otherwise there are primitive idempotents whose index is different from 1, and among those we choose a primitive idempotent e' of minimal index $m := |G_{e'}| > 1$. If then e is a primitive idempotent that corresponds to a character in the core of e' , we have $|G_e| < m$ by Proposition 3.7, and therefore $|G_e| = 1$. Since there are m such idempotents, one of them is different from the integral, which in view of the discussion above establishes our assertion. \square

It should be noted that the Nichols-Zoeller theorem for Yetter-Drinfel'd Hopf algebras cited in Paragraph 1.5 implies in this situation that the dimension of B divides the dimension of A .

References

- [1] N. Andruskiewitsch/H.-J. Schneider: Hopf algebras of order p^2 and braided Hopf algebras of order p , J. Algebra 199 (1998), 430–454
- [2] M. Beattie: On the Blattner-Montgomery duality theorem for Hopf algebras. In: D. Haile/J. Osterburg (ed.): Azumaya algebras, actions, and modules, Proceedings of a conference in honor of Goro Azumaya's seventieth birthday, Contemp. Math., Vol. 124, Am. Math. Soc., Providence, 1992, 23–28

- [3] C. W. Curtis/I. Reiner: Methods of representation theory with applications to finite groups and orders, Vol. I, Wiley, New York, 1981
- [4] Y. Doi: Unifying Hopf modules, *J. Algebra* 153 (1992), 373–385
- [5] Y. Doi: Hopf modules in Yetter-Drinfeld categories, *Commun. Algebra* 26 (1998), 3057–3070
- [6] B. Farb/R. K. Dennis: Noncommutative algebra, *Grad. Texts Math.*, Vol. 144, Springer, Berlin, 1993
- [7] D. Fischman/S. Montgomery/H.-J. Schneider: Frobenius extensions of subalgebras of Hopf algebras, *Trans. Am. Math. Soc.* 349 (1997), 4857–4895
- [8] M. Graña: A freeness theorem for Nichols algebras, *J. Algebra* 231 (2000), 235–257
- [9] B. Huppert: Endliche Gruppen I, *Grundlehren Math. Wiss.*, Vol. 134, Springer, Berlin, 1967
- [10] A. Joyal/R. Street: Braided tensor categories, *Adv. Math.* 102 (1993), 20–78
- [11] C. Kassel: Quantum groups, *Grad. Texts Math.*, Vol. 155, Springer, Berlin, 1995
- [12] H. Kurzweil/B. Stellmacher: The theory of finite groups, *Universitext*, Springer, Berlin, 2004
- [13] T. Y. Lam: A first course in noncommutative rings, *Grad. Texts Math.*, Vol. 131, Springer, Berlin, 1991
- [14] R. G. Larson/D. E. Radford: Semisimple cosemisimple Hopf algebras, *Am. J. Math.* 110 (1988), 187–195
- [15] R. G. Larson/D. E. Radford: Finite dimensional cosemisimple Hopf algebras in characteristic 0 are semisimple, *J. Algebra* 117 (1988), 267–289
- [16] F. W. Long: The Brauer group of dimodule algebras, *J. Algebra* 30 (1974), 559–601
- [17] V. Lyubashenko: Tangles and Hopf algebras in braided categories, *J. Pure Appl. Algebra* 98 (1995), 245–278
- [18] V. Lyubashenko: Modular transformations for tensor categories, *J. Pure Appl. Algebra* 98 (1995), 279–327
- [19] S. Montgomery: Hopf algebras and their actions on rings, 2nd revised printing, *Reg. Conf. Ser. Math.*, Vol. 82, Am. Math. Soc., Providence, 1997
- [20] W. D. Nichols/M. B. Zoeller: A Hopf algebra freeness theorem, *Am. J. Math.* 111 (1989), 381–385

- [21] D. E. Radford: The structure of Hopf algebras with a projection, *J. Algebra* 92 (1985), 322–347
- [22] D. E. Radford: Hopf algebras, Ser. Knots Everything, Vol. 49, World Scientific, Singapore, 2012
- [23] B. Scharfschwerdt: Endlich dimensionale Yetter-Drinfeld-Hopfalgebren, Dissertation, München, 2000
- [24] B. Scharfschwerdt: The Nichols-Zoeller theorem for Hopf algebras in the category of Yetter Drinfeld modules, *Commun. Algebra* 29 (2001), 2481–2487
- [25] P. Schauenburg: On the braiding on a Hopf algebra in a braided category, *New York J. Math.* 4 (1998), 259–263
- [26] Y. Sommerhäuser: Deformierte universelle Einhüllende, Diplomarbeit, München, 1994
- [27] Y. Sommerhäuser: Deformed enveloping algebras, *New York J. Math.* 2 (1996), 35–58
- [28] Y. Sommerhäuser: Ribbon transformations, integrals, and triangular decompositions, *J. Algebra* 282 (2004), 423–489
- [29] Y. Sommerhäuser: Yetter-Drinfel'd Hopf algebras over groups of prime order, Dissertation, München, 1999
- [30] Y. Sommerhäuser: Yetter-Drinfel'd Hopf algebras over groups of prime order, *Lect. Notes Math.*, Vol. 1789, Springer, Berlin, 2002
- [31] M. E. Sweedler: Integrals for Hopf algebras, *Ann. Math.*, II. Ser. 89 (1969), 323–335
- [32] M. E. Sweedler: Hopf algebras, Benjamin, New York, 1969
- [33] M. Takeuchi: Survey of braided Hopf algebras. In: N. Andruskiewitsch/W. R. Ferrer Santos/H.-J. Schneider (ed.): *New trends in Hopf algebra theory*, Proceedings of the colloquium on quantum groups and Hopf algebras, *Contemp. Math.*, Vol. 267, Am. Math. Soc., Providence, 2000, 301–323
- [34] V. G. Turaev: Quantum invariants of knots and 3-manifolds, de Gruyter Stud. Math., Vol. 18, de Gruyter, Berlin, 1994